Comptroller of the Currency
Administrator of National Banks

# Internal and External Audits

## Comptroller's Handbook

July 2000

M

Management

# Internal and External Audits Table of Contents

# Overview

## Background

Well-planned, properly structured auditing programs are essential to strong risk management and comprehensive internal control systems.[1] Effective internal and external audit programs are also a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal control systems.

OCC examiners will assess and draw conclusions about the adequacy of internal and external audit as part of every national bank examination. This will include some level of audit validation, including verification procedures as necessary. The conclusions will significantly influence the scope of other supervisory activities at the bank. The OCC will expand examination activities if significant issues are identified that require further investigation.

The following guidelines govern the assessment of national bank audit programs:

- The board of directors and senior management cannot delegate their responsibilities for establishing, maintaining, and operating effective audit programs.

- Bankers and examiners must each verify the adequacy of a national bank's audit programs.

- Bank audit programs will be performed by independent and competent staff who are objective in evaluating the bank's control environment.

This booklet discusses the characteristics of effective audit functions and will help examiners and bankers assess the quality and effectiveness of internal

[1] For a detailed description of internal controls, please refer to the *Comptroller's Handbook* booklet "Internal Controls" published in August 1988. The "Internal Controls" and the "Internal and External Audits" booklets supplement the core assessment standards in the "Large Bank Supervision" and "Community Bank Supervision" booklets of *the Comptroller's Handbook*. Further guidance on assessing controls can also be found in other *Comptroller's Handbook* booklets that address specific banking products and activities.

and external audit programs. It describes the roles and responsibilities of the board of directors and management, identifies effective practices for internal and external audit programs, and details examination objectives and procedures that OCC examiners will use to assess the adequacy of a national bank's audit programs. This booklet's appendixes provide additional guidance on internal and external audits.

***The examination procedures and other reference material in this booklet supplement the basic audit guidance in the "Community Bank Supervision" and "Large Bank Supervision" booklets of the* Comptroller's Handbook.**

## Audit Objectives

Effective audit programs:

- Provide objective, independent reviews and evaluations of bank activities, internal controls, and management information systems (MIS).
- Help maintain or improve the effectiveness of bank risk management processes, controls, and corporate governance.
- Provide reasonable assurance about the accuracy and timeliness with which transactions are recorded and the accuracy and completeness of financial and regulatory reports.

Audit programs may comprise several individual audits that provide various types of information to the board of directors about the bank's financial condition and effectiveness of internal control systems. The most common types of audits are financial, operational, compliance, and information systems or technology audits.

***Financial audits*** review an institution's financial statements, a specific account, or a group of accounts within the financial statements. The purpose of this audit is to determine whether the financial statements fairly present the financial position, results of operations, and cash flows as of a certain date or for a period ending on that date. Independent public accountants (IPAs)[2]

[2] Independent public accountants (IPAs) are accountants who are independent of the institutions they audit, are registered or licensed to practice accounting, hold themselves out as public accountants, and are in good standing under the laws of the state or other political subdivision of the United States in which their home office is located.

perform this type of audit primarily to render an opinion about whether the financial statements are presented fairly and in accordance with generally accepted accounting principles (GAAP). An internal auditor may assist the external auditor during such an audit.

***Operational audits*** review a specific department, division, or area of a bank. This type of audit includes a review of policies, procedures, and operational controls (e.g., loan review) to determine whether risk management, internal controls, and internal processes are adequate and efficient. Operational audits generally include procedures to test integrity of accounts, regulatory reports, and other aspects of operations. These audits may also include a review of management and employee compliance with bank policies and procedures. An audit of a bank's fiduciary activities is an example of an operational audit.

***Compliance audits*** determine whether the bank is complying with bank procedures, internal controls, and applicable laws and regulations. A consumer compliance audit is a typical example of this type of audit.

***Information system or technology audits*** assess the controls over an institution's electronic data processing and computer areas. These audits focus on management, development and acquisition, support and delivery, data security, and physical security. Information system or technology audits might also include a review of computer and client/server systems, end-user reports, electronic funds transfer, and service provider activities.

National bank audit programs should include each of these types of audits, although the level of formality and detail will vary. Auditors may perform these audits separately or blend elements of each to achieve overall bank audit objectives. In some institutions, the external auditors may perform some of the work that is traditionally thought to be internal audit work or rely on the work of the internal auditor. In small banks, individuals who have operational responsibilities may perform the internal audits in areas for which they have no responsibilities or involvement. Regardless of who performs the work, the institution's size, complexity, scope of activities and risk profile should determine the extent of its audit program.

## Regulatory Requirements

The following laws and regulations[3] establish minimum requirements for internal and external audit programs:

- 12 CFR 30, Safety and Soundness Standards, establishes standards for internal audit systems for insured national banks.

- 12 CFR 363, Annual Independent Audits and Reporting Requirements, applies to banks, thrifts, and holding companies having $500 million or more in total assets. Part 363 establishes requirements for independent financial statement audits; timing, content, and types of management and auditor reporting; and the board of director's audit committee structure and responsibilities.

- 17 CFR 210, 228, 229, and 240 are regulations of the Securities and Exchange Commission (SEC). These regulations require affected banks and holding companies to have their financial statements audited by an independent public accountant and impose specific requirements on audit committees.

- 12 CFR 9, Fiduciary Activities of National Banks, establishes an annual audit requirement for national banks acting in a fiduciary capacity and defines requirements for a bank's fiduciary audit committee.

The federal financial regulatory agencies have also issued three interagency policy statements on internal and external audit functions — "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing," "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," and "Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners." The policy statements discuss characteristics of effective internal and external audit programs, director and senior management responsibilities, and communication between external auditors and examiners.[4]

---

[3] Appendix A contains a more detailed description of the requirements of these laws and regulations. For complete details, refer to the full text of published laws and regulations.

[4] Appendices B, C, and D provide the full text of the policy statements.

## OCC Audit Supervision

Assessments of a national bank's audit programs are fundamental to the OCC's overall supervisory process. Audit assessments help leverage OCC resources, establish the scopes of other current supervisory activities, and contribute to supervisory strategies that outline future examination activity. The bank's examiner-in-charge (EIC) will tailor the scope of the audit examination to fit the bank's size, complexity, scope of activities, and risk profile.

### Supervisory Principles

Effective OCC audit supervision encompasses the following six principles:

**Integration**. The EIC should integrate audit reviews, including validation, into the supervisory activities for each functional, specialty, and risk area as needed. OCC specialists should be consulted about the audit functions for complex activities or should assist in assessing those activities. Examiners should use core assessment standards and other tools in assessing and documenting conclusions about individual areas and combining conclusions into an overall audit assessment.[5]

**Analysis**. An examiner should review audit reports and management responses, audit committee minutes records, and supervisory findings to identify changes in the bank's risk profile, systemic control issues, or changing audit trends. This review should also include other information maintained by the internal auditor, such as organization charts, audit charter or mission statement, external auditor or outsourcing vendor engagement letters, audit manuals, operating instructions, job specifications and descriptions, directives to employees, flow charts, and internal control and risk assessments.

**Communication**. OCC staff will maintain ongoing and clear communications with bank personnel. In large banks, the EIC or designee should have periodic meetings with a bank's audit committee and regular meetings with audit management/staff, other bank personnel closely associated with risk control functions (e.g., risk managers, control officers), and external auditors. While this degree of contact may not be practical for all community banks, meetings with audit committees and internal and external audit personnel should occur

[5] Appendix E provides a sample internal audit review worksheet which can assist examiners in making an overall internal audit assessment.

as appropriate depending on the bank's size, complexity, scope of activities, and risk profile. Communication regarding audit supervision and audit findings should occur throughout an examination or supervisory cycle. Examination reports and other written communications to a bank will include comments about the adequacy of the bank's audit programs and summarize other appropriate findings and conclusions.

**Linkage**. Examiners should link audit conclusions to assigned bank ratings, risk assessments, and supervisory strategies. In particular, management ratings, audit component ratings in the specialty areas, and individual risk assessments should be linked directly to the quality and reliability of a bank's audit functions.

**Documentation**. The examiner should document working papers in accordance with OCC working paper guidelines (PPM 5400-8, "Examination Working Papers"). Working papers need not be voluminous, but they should leave a clear audit trail that supports findings and conclusions and allows the EIC or another reviewer to understand how conclusions were reached. Examiners will also update OCC databases and supervisory strategies to reflect supervisory assessments and follow-up.

**Interagency coordination**. Audit supervision may involve working with Federal Reserve examiners in bank holding company situations, Federal Deposit Insurance Corporation (FDIC) examiners in problem bank situations, or other functional supervisory agencies such as the SEC. In such cases, the EIC should coordinate the timing of audit reviews and share information with the appropriate supervisory agencies. Examiners participating in joint holding company examinations should, after consultation with the Federal Reserve, communicate audit conclusions to affiliate national bank EICs.

## Supervisory Process and Validation

OCC examiners will draw an overall conclusion and assess as strong, satisfactory, or weak the adequacy of the bank's internal and external audit programs during every supervisory cycle. The supervisory assessment of the audit program will influence how much work examiners will perform during on-site examinations. In developing the appropriate scope for audit activities, community bank examiners will begin with the core assessment objectives and procedures in the "Community Bank Supervision" booklet. Large bank examiners will begin with the minimum audit standards in the "Large Bank

Supervision" booklet and tailor their review, using objectives and procedures in this booklet, to fit the size, complexity, scope of activities, and risk profile of the institution being examined.

Examiners responsible for audit program reviews will determine how much reliance the OCC can place on internal and external audit work by validating the audit program at each regular on-site examination. The objective of the OCC's validation work is to gain a better understanding of audit-related policies, procedures, practices, and findings, and to substantiate conclusions about the quality and reliability of internal and external audits.

Validation encompasses observation, inquiry, and testing and generally consists of a combination of examiner discussions with bank management and audit personnel, audit work paper reviews, and process reviews (e.g., reviews of policy adherence, risk assessments, follow-up activities).

*To validate the adequacy of the bank's audit program, OCC examiners may progress through three steps:* ***work paper review****,* ***use of additional procedures****, and* ***direct verification****.*

**Work paper review**. During each supervisory cycle, examiners will review an appropriate sample of internal audit program work papers, including those from outsourced internal audit work and directors' examinations. The sample for internal audit work paper reviews should represent a cross-section of bank functions, activities, and assigned internal audit ratings, with a bias toward high-risk and rapid growth areas, technology audits, and activities that are new to the bank. The sample should provide a sufficient basis to validate the scope and quality of the audit programs.

For community banks with relatively low complexity and internal audit functions previously assessed at least satisfactory, the extent of work paper reviews may be limited to confirming that the audit program has not changed substantially since the last examination.

If the examination discloses significant problems or issues with external audit, or if examiners become aware of information that raises questions about the adequacy of the external audit program, examiners should review appropriate external audit work papers. Examples of situations that might trigger an external audit work paper review are:

- Bank reliance on external audit in lieu of an internal audit program.
- Unexpected or sudden changes in the external auditor.
- Significant changes in the external audit program.
- Significant safety and soundness concerns.
- Issues about independence, objectivity, or competence of the external auditor.

For external audits conducted at banks subject to 12 CFR 363, IPAs are required to provide the OCC access to audit-related work papers, policies, and procedures upon request. Examiners should initially request access to such audit work papers through bank management, but should not hesitate to communicate directly with the external auditor if bank management fails to provide access.[6]

For banks that have outsourced internal audit activities or external audit programs not subject to 12 CFR 363, engagement letters or written contracts should explicitly provide for examiner access to audit work papers in accordance with interagency policy statements.

An IPA may request that examiners view external audit work papers at the IPA's office. The IPA may also require that their representative(s) be present during the reviews and may not allow photocopying. Examiners' request for work papers should be specific to the areas of greatest interest and set forth the reason for the request. When the audit work papers support holding company financial statement audits or attestation reports, examiners should coordinate reviews with appropriate OCC supervisory offices and other regulators. Because the IPA or outsourced vendor may bill the bank for time spent by IPA staff in conjunction with an examiner's review of external audit or outsourced internal audit work papers, the review should be focused and efficient.

**Use of Additional Procedures**. If the audit work paper review identifies significant discrepancies or weaknesses in the audit function, examiners will expand the examination of the audit program and determine, with the EIC, if the examination work in affected operational or functional business area(s) should also be expanded. For example, examiners will expand audit program procedures if they encounter or identify:

[6] Examiners should refer to the July 1994 AICPA interpretation of Statement on Auditing Standard (SAS) 41, *Working Papers*, entitled "Providing Access to or Photocopies of Working Papers to a Regulator" in the AICPA's *Professional Standards.*

- Issues of competency or independence relating to internal or external auditors.

- Unexplained or unexpected changes in external auditor or significant changes in the audit program.

- Inadequate scope of the audit program.

- Audit work papers that are deficient or do not support audit conclusions.

- High growth areas of the institution without adequate audit or internal controls.

- Inappropriate actions by insiders to influence the findings or scope of audits.

The scope of work must be sufficient to determine the extent of problems and their effect on bank operations. Examiners should include appropriate internal control questionnaires (ICQs) in the expanded procedures.

**Direct Verification**. If after completion of the expanded procedures, concerns remain about the adequacy of audit, internal controls, or the integrity of the bank's financial controls, examiners should use verification procedures to substantiate the internal or external auditor's work. Verification should include, but not be limited to, direct confirmations with customers, servicers, and others as appropriate. Examiners should consult with their supervisory office or the Chief Accountant's office before conducting direct confirmations. Examiners will perform verification even in situations in which the external auditor has issued an unqualified opinion if discrepancies or weaknesses call into question the accuracy of the opinion.

Verification procedures must be used whenever:

- Account records are significantly out of balance.

- Management is uncooperative or poorly manages the bank.

- Management restricts access to bank records.

- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.

- Bank auditors are unaware of, or unable to sufficiently explain, significant deficiencies.

- Management engages in activities that raise questions about its integrity.

- Repeated violations of law affect audit, internal controls, or regulatory reports.

- Other situations exist that examiners believe warrant further investigation.

For less problematic situations than those identified above, the examiner may require the bank to expand its audit program to include the areas containing weaknesses or deficiencies. However, this alternative will only be used if management has demonstrated a capacity and willingness to address regulatory problems, if there are no concerns about management's integrity, and management has initiated timely corrective action in the past. If used, this alternative must resolve each identified supervisory problem in a timely manner. If examiners use this alternative, supervisory follow-up will include a review of audit work papers in areas where the bank audit was expanded.

## Audit Evaluation

The remaining sections of this booklet discuss characteristics and practices of effective internal and external audit programs. Examiners will evaluate the extent to which the bank uses these practices in light of the bank's size, complexity, scope of activities, and risk profile. During each bank's supervisory cycle, examiners will evaluate the quality and scope of the audit program considering whether:

- The board of directors or its audit committee reviews and approves audit policies at least annually.

- The board of directors or its audit committee monitors the implementation of the audit program and its audit schedule.

- The internal and/or external audit functions are sufficiently independent and their staffs are competent.

- The audit's scope and frequency, risk assessments, plans, and work programs are appropriate.

- Audit findings are promptly communicated to the board of directors or its audit committee and appropriate bank management.

- The board and management properly follow up on the results of audits and appropriately monitor any significant issues.

- Internal and/or external auditors maintain an appropriate level of professional standards and training/development.

Examiners should contact OCC district management, the Chief Accountant's Office, or the Chief Counsel's Office, as appropriate, when significant questions arise regarding the independence, objectivity, or competence of the bank's external or outsourced internal auditors given their importance to the overall audit assessment. These discussions should take place prior to discussing the issues with the board of directors, senior management, audit management, or the external auditor.

When warranted by the circumstances, the OCC may refer an external auditor to the state board of accountancy or the American Institute of Certified Public Accountants (AICPA) for possible ethics violations. If necessary, the OCC may also bar an external auditor from engagements with OCC-supervised institutions. Examiners should direct questions about such referrals to district management, the Chief Accountant's office, or the Chief Counsel's Office.

At the conclusion of the audit review, the EIC or designee will discuss significant audit weaknesses or audit-related recommendations with audit management and with the board of directors and thereafter prepare a summary of the discussions for the examination working papers. Examiners also will prepare comments, including "Matters Requiring Attention" if applicable, for the Report of Examination. The comments should summarize the adequacy of the bank's audit program and identify any significant audit issues or concerns.

If significant audit weaknesses are identified, the EIC will determine whether to recommend to the appropriate supervisory office that bank management

develop a compliance plan, consistent with 12 CFR 30, to address the weaknesses or be subject to other types of enforcement actions. In making a decision, the supervisory office will consider the significance of the weaknesses, management's ability and commitment to effect corrective action, and the risks posed to the bank.

## Board and Management Oversight

A bank's board of directors is responsible for establishing and maintaining effective audit functions that satisfy statutory, regulatory, and supervisory requirements. Directors cannot delegate these responsibilities. However, they may delegate the design, implementation, and monitoring of specific internal controls to management and the testing and assessment of internal controls to auditors and others. Board or audit committee minutes should reflect decisions regarding audits, such as external audit engagement terms (including any decision to forgo an external audit), the scope of audits to be performed, or why an audit of a particular area is not necessary.

Directors are specifically responsible for reviewing and approving audit strategies, policies, programs, and organizational structure. They should also monitor the effectiveness of the audit function.

The formality and extent of an institution's internal and external audit programs depend on the bank's size, complexity, scope of activities, and risk profile. Some small banks do not have either a formal internal or external audit program. Instead, audit responsibilities may lie with an officer or employee designated as a part-time auditor or with employees who may share the audit tasks. In other banks, the board, through its annual director's examination, performs the external audit function.

The board of directors must carefully consider how extensive the audit program must be to effectively test and monitor internal controls and ensure the reliability of the bank's financial statements and reporting. The directors (and audit management if the bank employs them) must ensure that the bank's audit programs test internal controls to identify:

- Inaccurate, incomplete, or unauthorized transactions;
- Deficiencies in the safeguarding of assets;
- Unreliable financial and regulatory reporting;
- Violations of laws or regulations; and

- Deviations from the institution's policies and procedures.

While 12 CFR 363 requires national banks holding more than $500 million in assets to have an audit committee consisting entirely of outside directors, the OCC encourages all other national banks to have a similarly structured audit committee. In small banks where this may not be practical, outside directors should be at least a majority of the audit committee.

The SEC also imposes specific requirements on audit committees aimed at strengthening their independence, effectiveness, and accountability. In registered national banks, the audit committees might be required to comply with 12 CFR 363 and other SEC rulings.

At least annually, audit management should identify the major risks faced by the bank to assist the board of directors or the audit committee in establishing appropriate audit coverage. The board or audit committee should also ensure that internal and external auditors are independent of bank management and are objective. The audit committee normally should be involved in hiring senior internal audit personnel, setting compensation for internal audit staff, reviewing audit plans, and evaluating the performance of internal auditors. It should seek to retain personnel who are qualified to audit the activities in which the bank engages, evaluate internal controls, and determine whether management is properly following up on the auditor's or the OCC's recommendations and concerns. The committee also may meet with examiners as necessary to review reports and discuss findings.

Under 12 CFR 9, a bank's fiduciary audit committee must consist of only its own directors or it must be a committee of one of the bank's affiliates. Officers of the bank or an affiliate who participate significantly in the administration of the bank's fiduciary activities cannot serve on the fiduciary audit committee. Additionally, a majority of the committee's members cannot be members of a committee that manages or controls any of the bank's fiduciary activities.

Directors must be aware of all risks and control issues for the bank's operations, including risks in new products, emerging technologies, information systems, and electronic banking. Control issues and risks associated with increasing reliance on technology include increased user access to information systems, reduced segregation of duties, a shift from paper to electronic audit trails, a lack of standards and controls for end-user

systems, and increased complexity of contingency plans and information system recovery plans.

Audit management is responsible for implementing board-approved audit directives. They oversee audit operations and provide leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. Audit management should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. They also should ensure that members of the audit staff possess the necessary experience, education, training, and skills to properly conduct assigned activities.

## Risk Assessment and Risk-based Auditing

The OCC, with the other federal banking regulators, encourages risk assessment and risk-based auditing for all banks. Risk assessment is the means by which a bank identifies and evaluates the quantity of the bank's risks and the quality of its controls. Through risk-based auditing, the board and auditors use the results of the risk assessments to focus on the areas of greatest risk and to set priorities for audit work. **An effective risk-based auditing program will cover all of a bank's activities. The frequency and depth of each area's audit will vary according to the area's risk assessment.**

### Program Elements

Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of risk-based audits will vary for individual banks depending on the bank's size, complexity, scope of activities, capabilities of bank staff, quality of control functions, geographic diversity, and technology used. All risk-based audit programs should:

- Identify all of an institution's businesses, product lines, services, and functions.

- Identify the activities within those businesses, product lines, services, and functions that the bank should audit.

- Include profiles of significant business units, departments, and products that identify business and control risks and document the structure of risk management and internal control systems.

- Use a measurement or scoring system to rank and evaluate business and control risks of significant business units, departments, and products.

- Include a risk-based audit plan that establishes audit schedules, audit cycles, work program scope, and resource allocation for each area to be audited.

- Implement the audit plan through planning, execution, reporting, and follow-up.

- Have systems that monitor risk assessments regularly and update them at least annually for all significant business units, departments, and products.

## Risk Scoring System

An effective scoring system is critical to a successful risk-based audit program. In establishing a scoring system, the directors and management must consider all relevant risk factors so that the system minimizes subjectivity, is understood, and is meaningful. Major risk factors commonly used in scoring systems include the nature of transactions (e.g., volume, size, liquidity); the nature of the operating environment (e.g., complexity of transactions, changes in volume, degree of system and reporting centralization, economic and regulatory environment); internal controls, security, and MIS; human resources (e.g., experience of management and staff, turnover, competence, degree of delegation); and senior management oversight of the audit process.

Directors should approve written guidelines on the use of risk assessment tools and risk factors. The sophistication and formality of guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and technology used. Auditors will use the guidelines to grade or assess major risk areas. These standards generally define the basis for the bank's weights and scores (e.g., the basis could be normal industry practices or the bank's own experiences). They also define the range of scores or assessments (e.g., low, medium, and high, or a numerical sequence, for example, 1 through 5). The written guidelines should specify:

- The length of the audit cycles based on the scores or assessments. Audit cycles should not be open-ended. For example, some banks set audit cycles at 12 months or less for high-risk areas, 24 months or less for medium-risk areas, and more than 24 months for low-risk areas. However, individual judgment and circumstances at each institution will determine the length of its audit cycles.

- Guidelines for when risk assessments can be overridden, who has override approval authority (i.e., board, audit committee, or audit management), and for reporting and documenting overrides. Overrides of risk assessments should be more the exception than the rule.

- The timing of risk assessments for each department or activity. Normally risks are assessed annually, but they may need to be assessed more often if the bank or a bank product experiences excessive growth or bank staff or activities change significantly.

- Minimum documentation requirements to support scoring or assessment decisions.

Banks can obtain matrices, models, or additional information on risk assessments from industry groups such as the American Bankers Association, AICPA, Institute of Internal Auditors (IIA), Financial Managers Society, and many certified public accounting firms. Another resource for helping directors and auditors evaluate controls and risk assessments is the "Internal Control – Integrated Framework" report issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Day-to-day management of the risk-based audit program rests with the internal auditor or internal audit manager who will monitor the audit scope and risk assessments to ensure that audit coverage remains adequate. The internal auditor or audit manager will also prepare reports showing the risk rating, planned scope, and audit cycle for each area. The audit manager should confirm the risk assessment system's reliability at least annually or whenever significant changes occur within a department or function.

Line department managers and auditors should work together in evaluating the risk in all departments and functions. Line department managers should review risk assessments to determine whether they are reasonable. Auditors periodically review the results of internal control processes and analyze

financial or operational data for any effect on a risk assessment or weighting. Accordingly, bank management should keep auditors current on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, or changes in organization or staff.

## Internal Audit Function

The primary role of the internal auditor is to independently and objectively review and evaluate bank activities to maintain or improve the efficiency and effectiveness of a bank's risk management, internal controls, and corporate governance. Internal auditors must understand a bank's strategic direction, objectives, products, services, and processes. The auditors communicate findings to the board of directors or its audit committee and senior management.

### Objectives

The objectives of internal audit are to:

- Evaluate the reliability, adequacy, and effectiveness of accounting, operating, and administrative controls.

- Ensure that bank internal controls result in prompt and accurate recording of transactions and proper safeguarding of assets.

- Determine whether a bank complies with laws and regulations and adheres to established bank policies, and whether management is taking appropriate steps to address control deficiencies.

Internal auditors are increasingly responsible for providing constructive business advice on adding new products or services. They also help the bank formulate new policies, procedures, and practices and revise existing ones. Internal auditors often have a role in merger, acquisition, and transition activities. This role includes helping the board and management evaluate safeguards and controls, including appropriate documentation and audit trails, during the bank's acquisition planning and implementation processes.

## Oversight and Structure

Institutions should conduct their internal audit activities according to existing professional standards. The IIA's "Standards for the Professional Practice of Internal Auditing" establish standards for independence, professional proficiency, scope of work, performance of audit work, and management of internal auditing.[7] The Bank Administration Institute (BAI) has adopted the IIA's standards for certified bank auditors. Internal auditors who are not certified or IIA members should be familiar with these or similar standards.

How an internal audit function is organized depends on the bank's size, complexity, scope of activities, and risk profile, as well as the audit function's board-assigned responsibilities. In larger banks, the chief auditor is often a manager who fulfills his or her responsibilities with the help of an audit staff. The internal audit function also can be performed by bank or holding company employees or by an outside vendor. In many small banks, an officer or employee designated a part-time auditor may have operational responsibilities. To maintain independence, the employee reviewing a particular function should be independent of that function and should report findings directly to the board or its audit committee.

## Internal Audit Program

A national bank's internal audit program consists of the policies and procedures that govern its internal audit functions, including risk-based auditing programs and outsourced internal audit work, if applicable. While smaller banks' audit programs may not be as formal as those found in larger, more complex banks, all audit programs include the following:

- ***Mission statement or audit charter that outlines the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit department, audit staff, and the audit committee.***

- ***Risk assessments that document the bank's significant business activities and their associated risks.*** Results of these risk assessments guide the development of an audit plan and audit cycle and the scope and objectives of individual audit programs. The "Risk Assessment and Risk-based

[7] Those standards and other material about the practice of internal auditing can be found at the IIA's Web site (www.theiia.org).

Auditing" section of this booklet provides further details on risk assessments.

- ***An audit plan that details an internal auditor's budgeting and planning processes.*** The plan should describe audit goals, schedules, staffing, and reporting. Audit plans usually include overall and individual audit objectives, summary risk assessments for each audit area or business activity, the timing and frequency of planned internal audit work, and a resource budget (budgeted staff hours). The audit committee should formally approve the audit plan at least annually. The internal auditor should present any updated audit plan to the audit committee regularly (in accordance with established policy, although quarterly is typical). Updated audit plans should compare actual with planned audits and audit hours and explain significant variances from the approved plan.

- ***An audit cycle that identifies the frequency of audits.*** The frequency of audits is usually determined by risk assessments of business activities or areas to be audited and the staff and time available. It is often not practical to audit each area or business activity annually. Areas of high risk, such as funding, lending, or investment/treasury operations, normally warrant more frequent audits than low-risk areas such as bank premises. Additionally, auditors must consider regulatory and supervisory requirements and guidelines.

- ***Audit work programs that set out, for each audit area, the scope and timing of audit procedures, the extent of testing (including criteria for selecting items to be tested), and the basis for conclusions.*** Work programs should be detailed, cover all areas of the bank's operation, and guide the auditor in gathering information, documenting procedures performed, arriving at conclusions, and issuing the audit reports. By completing the audit work programs, an internal auditor should be able to reach conclusions that satisfy internal audit objectives. Work programs normally include procedures for:

  - Surprise audits as appropriate.
  - Control over records selected for an audit.
  - Review and evaluation of policies, procedures, and control systems.
  - Risk assessments.
  - Review of laws, regulations, and rulings.
  - Sample selection methods and results.

– Verification of selected transactions or balances through:
  - Proof of subsidiary records/ledgers to related general ledger/control records.
  - Examination of supporting documentation.
  - Direct confirmation and appropriate follow-up for exceptions.
  - Physical inspection.

As part of audit work programs, auditors generally use **sampling methods and techniques** to select, verify, and test transactions, controls, and account balances for the period covered by the audit review. The audit work program should determine the objectives of testing, the procedures to meet the objectives, and how many items to review (i.e., all items in a group or a sample of items). When auditors choose to review a sample, they must decide whether to use statistical or nonstatistical sampling methods. Auditors often use nonstatistical sampling for small populations when internal controls are effective and it is not cost-effective to use statistical sampling. Auditors use statistical sampling methods when quantification is appropriate and they want to infer with a certain degree of reliability and precision that the sample's characteristics are indicative of the entire population. In either case, the auditor determines a representative sample size based on relevant factors, selects a representative sample, applies audit procedures, evaluates results, and documents conclusions. There are no hard and fast rules regarding the appropriate size of a "representative sample." Published tables provide statistical sample sizes based on desired precision and reliability levels. When assessing audit sampling processes, examiners will review the auditor's documentation relating to sampling objectives, including procedures for establishing sampling objectives, defining population and review characteristics, determining sample size, selecting sample methodology, and evaluating sample results/findings.[8]

- ***Audit reports that tell the board and management whether a department, division, or activity adheres to policies and procedures, whether operating processes and internal controls are effective, and what corrective action the bank has taken or must take.*** The auditor must communicate findings and recommendations to appropriate parties and distribute audit reports as soon as practical after completing the related

[8] The "Sampling Methodologies" booklet of the *Comptroller's Handbook* more fully describes the concepts behind statistical sampling methods. In addition, the auditing industry (i.e., accounting firms, IIA, BAI, et al) also addresses audit sampling issues in audit manuals and other guidance.

work. Audit work papers should adequately document and support these reports.

Internal audit reports should be structured to fit the needs of a bank's internal audit function and the areas being audited. The reports usually contain the following information:

- A concise summary of key results and conclusions.
- The audit's scope and objectives.
- Audit results, including any summary rating.
- Recommendations, if any, including benefits to be derived.
- Management's commitments to correct material weaknesses.

After completing an audit, the internal auditor usually meets with the manager of the department to review the draft audit report, correct any inaccurate information, and reach agreement on management's commitments and actions. A final audit report is then distributed to the management officials who have the responsibility and authority to implement any suggested corrective actions.

- ***Follow-up activities that allow internal auditors to determine the disposition of any agreed-upon actions and to focus future audit activities on new areas.*** The auditors should perform follow-up activities promptly and report the results to the board of directors or its audit committee. Follow-up generally consists of first obtaining and reviewing management's response and then confirming that corrective action has been timely and effective.

- ***Professional development programs for the bank's audit staff.*** Such programs should offer opportunities for continuing education and professional development through orientation programs, in-house training, and external training (e.g., formal or self-study courses offered by industry associations, professional societies, or other vendors).

- ***Quality assurance programs, generally seen in large or mid-sized banks, which evaluate audit operations.*** In such programs, internal or external parties periodically assess the performance of the internal auditor or audit department. The auditor or audit department's performance is normally measured against bank-established standards, the audit charter or mission

statement, and any other criteria determined appropriate for the internal audit function.

## Independence

Internal auditors must be independent of the activities they audit so that they can carry out their work freely and objectively. They must render impartial and unbiased judgments. The internal auditor or the manager (director) of internal audit should report directly and regularly to the board of directors. In some banks, the internal audit function may be part of a group that manages or controls the bank's overall risk-taking activities. This arrangement may be satisfactory as long as the audit function reports directly to the board and retains its independence.

The board is responsible for delegating the authority necessary to effectively allow internal auditors to perform their job. Auditors must have the power to act on their own initiative in all departments, divisions, and functions in the bank; to communicate directly with any bank personnel; and to gain access to all records, files, or data necessary for the proper conduct of the audit. Clear communication between the board, the internal auditors, and management is critical to timely identification and correction of weaknesses in internal controls and operating management.

In some banks, the head auditor reports to a senior manager, rather than the board, for day-to-day administrative issues. In such a case, the board must take extra measures to ensure that the relationship does not impair or unduly influence the auditor's independence.

## Competence

Internal audit staff should possess the necessary knowledge, skills, and disciplines to successfully implement the audit program in a proficient and professional manner. The evolving roles of internal auditors require that they expand their skills in analysis, technology, decision-making, and communication. At a minimum, members of the audit staff should:

- Have appropriate education and/or experience.
- Have organizational and technical skills commensurate with the responsibilities assigned.

- Be skilled in oral and written communication.
- Understand accounting and auditing standards, principles, and techniques.
- Recognize and evaluate the materiality and significance of deviations from sound business practices.
- Recognize existing or potential problems and expand procedures as applicable.

It is important for each member of the internal audit staff, including the audit manager or director, to commit to a program of continuing education and development. Courses and seminars offered by colleges, bank groups, or audit industry groups afford many opportunities for maintaining audit skills and proficiency. They also offer a means to become certified as bank auditors, internal auditors, or public accountants. In-house training programs, work experience in various departments of a bank, and reviewing current literature on auditing and banking also are means to maintain and enhance auditing skills.

In a small bank, internal auditing may be a one-person department. Nevertheless, the auditor should possess qualifications similar to those outlined above.

## Outsourcing Internal Audit

Banks are increasingly contracting with independent public accounting firms or other outside professionals to perform work traditionally conducted by internal auditors. These arrangements are frequently referred to as "internal audit outsourcing," "internal audit assistance," "audit integration," "audit cosourcing," or "extended audit services." In any outsourcing arrangement, the bank should have a designated employee (generally an internal auditor or internal audit manager/director) who is independent and responsible for managing the relationship with the outside firm. Banks generally enter into internal audit outsourcing arrangements to gain operational or financial efficiencies by engaging a vendor to:

- Assist its internal audit staff when the bank's internal auditors lack the expertise required for an assignment. Such assignments are most often in

specialized areas such as information technology, fiduciary, mortgage banking, and capital markets activities. The vendor normally performs only certain agreed-upon procedures in specific areas and reports findings directly to the bank's internal audit manager.

- Perform the entire internal audit. The bank's only internal audit staff may be an audit manager. The vendor usually assists the board and audit manager in determining the critical risks to be reviewed during the engagement, recommends and performs audit procedures approved by the internal auditor, and, jointly with the internal auditor, reports significant findings to the board of directors or its audit committee.

Examiners assess outsourced internal audit programs using the same standards applied to internal audit programs. Outsourcing arrangements create a variety of safety and soundness issues that will vary with the size, complexity, scope of activities, and risk profile of the bank and the nature of the outsourcing arrangement. Accordingly, outsourced arrangements should meet the following guidelines:

- ***The arrangement maintains or enhances the quality of a bank's internal audit function and internal controls.*** The directors remain responsible for ensuring that any outsourcing arrangement is competently managed and does not detract from the scope or quality of a bank's internal audit work, overall internal control structure of the bank, or audit and control evaluations. The bank should subject the vendor to objective performance criteria such as whether an audit is completed on time and whether overall performance meets the objectives of the audit plan. The audit committee or a designated bank staff responsible for oversight should sample outsourced audit work to determine the adequacy of the vendor's work and compliance with contractual and coverage requirements.

- ***Key bank employees and the vendor clearly understand the lines of communication and how the bank will address internal control or other problems noted by the vendor.*** The engagement of a vendor should not diminish communication between the internal audit function and a bank's directors and senior management. Results of outsourced work must be well documented and reported promptly to the board of directors or its audit committee by the internal auditor, the vendor, or both jointly.

- ***The board and management perform sufficient due diligence to verify the vendor's competence and objectivity before entering into the outsourcing arrangement.*** The internal audit manager and the board of directors must be assured that a vendor can acceptably complete the work to be outsourced. They should be familiar with the AICPA's interpretation 102-2 about conflicts of interest under Rule 102 on integrity and objectivity of IPAs performing outsourced internal audit.

- ***The bank has adequate procedures for ensuring that the outside vendor maintains sufficient expertise to perform effectively throughout the life of the arrangement.*** The board of directors should hold the outside provider to the same standards as they would their own internal audit management and staff. Bank management should perform enough due diligence to be satisfied that the expertise and quality of the vendor's staff is sufficient to effectively meet contractual obligations. The vendor should provide the bank prior notice of any staffing changes affecting contracted work.

- ***The arrangement does not compromise the role or independence of a vendor who also serves as the bank's external auditor.*** The OCC discourages banks from outsourcing internal audit work to the same external audit firm that performs its financial statement audits and other attestation services. When one firm performs both jobs, the bank's board, management, the auditor, and the OCC must pay particular attention to independence issues.[9]

All national banks engaged in outsourcing internal audit activities must execute a written contract that governs the terms of the outsourcing arrangement and specifies the roles and responsibilities of both the bank and the vendor. At a minimum, the contract should: (1) set the scope and frequency of the vendor's work; (2) describe how and when the vendor provides results to the bank's audit manager, senior management, and the board; (3) describe how the terms of the engagement can be changed, including how audit services can be expanded when significant issues arise; (4) stipulate that the audit reports are the property of the bank, the bank can

[9] The AICPA has issued several interpretations (101-13) and rulings (101, 103, 104, and 105) regarding independence standards for outsourced audits (see appendix B). Some things that might compromise independence are: an IPA reporting to the board or audit committee on behalf of bank management or the individual responsible for the bank's internal audit function, an IPA acting or appearing to act as if he or she were bank management or a bank employee, or an IPA providing the primary support for bank management's assertion on financial reporting controls.

get copies of the vendor's work papers when it deems necessary, and bank employees have reasonable and timely access to vendor work papers; 5) state where work papers will be stored; (6) give OCC examiners immediate and full access to all outsourced audit reports and related work papers; and (7) establish a dispute resolution process for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.

## External Audit Function

While required by 12 CFR 363 for banks having $500 million or more in total assets, the OCC strongly encourages all other national banks to establish and maintain an external audit program. A well-planned external audit complements the bank's internal audit function, strengthens internal controls, and contributes to safe and sound operations. Many of the principles discussed below are highlights of broader requirements set forth in the AICPA's *Professional Standards* and *Audit and Accounting Guide, Banks and Savings Institutions*. The OCC encourages examiners and bankers to consult these source documents for more detail on specific standards and for guidance concerning the role of independent accountants.

Examiners will use judgment and discretion when evaluating a board's decision to forgo an external audit. OCC examiners will not criticize a small bank or include adverse comments in the Report of Examination simply because it does not have an external audit program. Examiners' considerations should include a bank's size; the nature, scope, and complexity of its activities; its risk profile; the extent of its internal audit program; compensating internal controls; and the significance of any identified audit or internal control weaknesses.

### Objectives

An effective external audit function provides the board of directors and management with:

- Reasonable assurance about the effectiveness of internal controls over financial reporting, the accuracy and timeliness in recording transactions, and the accuracy and completeness of financial and regulatory reports.

- An independent and objective view of a bank's activities, including processes relative to financial reporting.

- Information useful to directors and management in maintaining a bank's risk management processes.

External auditors often provide services throughout the year, including in-depth reviews of the operations of specific departments, such as commercial loans or data processing. Such reviews often focus on operational procedures, personnel requirements, or other specific areas of interest. Banks employ external auditors to help management in specialized fields such as taxes and management information systems. External auditors may, when requested, also help banks prepare or review call reports.

A bank's board of directors should require external auditors to submit engagement letters before commencing audit work. The letters usually reflect preliminary discussions between the bank's board or senior management and the external auditor. Engagement letters stipulate, among other things, the audit's purpose, its scope, the period to be covered, and the reports the external auditor will develop. Schedules or appendixes may accompany the letter to provide more detail. The letter may briefly describe procedures to be used in specific areas. In addition, if the scope of the audit is limited in any way, the letter may specify procedures that the auditors will omit. Additionally, the letter should specify if the auditor is expected to render an opinion on the bank's financial statements.

After an audit has taken place, external auditors often make suggestions for improving the bank's internal control structure. They normally do so in a letter addressed to bank management and the audit committee ("management letter") that is separate from the audit report. Statement on Auditing Standards (SAS) 60, "Communication of Internal Control Structure Related Matters Noted in an Audit," requires the auditor to communicate such matters to management, preferably in writing, and provides appropriate guidance.

The OCC encourages communication and cooperation between bank management, external auditors, and the OCC examination team. For specific guidelines on such communication, see the "Interagency Policy Statement on Coordination and Communication between External Auditors and Examiners" (appendix D) and the AICPA's *Audit and Accounting Guide, Banks and Savings Institutions*. Communication and cooperation can benefit all parties by helping to improve the quality of internal controls and bank supervision

while promoting a better understanding of the OCC's and the external auditor's policies and practices.

Examiners should consider contacting or meeting with external auditors during an examination, especially if there are questions or issues regarding the external audit. Topics of discussion should include examination and audit results or major findings; upcoming audit and examination activities; assessment of internal controls; reports, management letters, or documents; and other appropriate audit or supervisory topics.

## Types of External Auditing Programs

When the board of directors analyzes a bank's external auditing needs, it should decide which of the following types of external audits best fits its needs.

**Financial statement audit by an IPA.** External auditing is traditionally associated with independent audits of a bank's financial statements. An independent audit of financial statements is designed to ensure that financial reports are prepared in accordance with generally accepted accounting principles (GAAP). Independent financial statement audits are performed in accordance with generally accepted auditing standards (GAAS). Their scope is sufficient to enable an IPA to express an opinion on the bank's (or parent holding company's consolidated) financial statements. National banks with total assets of $500 million or more are required by 12 CFR 363 to have an IPA audit their financial statements.[10] The OCC encourages all other national banks to voluntarily engage the services of an IPA to conduct financial audits of the bank's financial statements.

**Reporting by an IPA on a bank=s internal control structure governing financial reporting.** This type of audit examines and reports on management's assertion concerning the effectiveness of the bank's internal controls over financial reporting. The IPA's attestation may cover all internal controls relating to annual financial statement preparation or specified schedules of call reports. Under this engagement, bank management documents its assessment of internal controls and prepares a written assertion specifying the criteria used and opining on control effectiveness. The IPA performs the attestation in

[10] The audited financial statements requirement of 12 CFR 363.2(a) can be satisfied for a bank that is a subsidiary of a holding company by audited financial statements of the consolidated holding company.

accordance with generally accepted standards for attestation engagements (GASAE).

**Balance sheet audit performed by an IPA.** In this type of audit, an IPA examines and reports only on the bank's balance sheet. As with financial statement audits, the IPA audits in accordance with GAAS, but does not examine or report on whether statements of income, changes to equity capital, or cash flow are fairly presented.

**Agreed-upon procedures.** This type of audit, carried out by bank directors or other independent parties, entails specified or agreed-upon procedural reviews of the adequacy of internal controls and the accuracy of financial information. Such an audit is commonly referred to as a directors' examination (see below). The independent parties can be public accountants, certified internal auditors, certified bank auditors, certified information systems auditors, bank management firms, bank consulting firms, or other parties knowledgeable about banking.

## Directors' Examinations

The bylaws of many national banks require that the directors have independent parties periodically examine the bank's affairs. In these cases, the board is responsible for determining that agreed-upon procedures adequately meet the bank's external auditing needs. The board considers such issues as the bank's size, complexity, scope of activities, and risk profile. Agreed-upon procedures normally focus on the bank's high-risk areas and consist of more than just confirmations of loans and deposits. After reviewing the findings of this type of review, the board or audit committee draws its own conclusions about the quality of financial reporting and adequacy of internal controls.

The report of examination findings, also commonly known as a director's examination, usually states whether the bank is in sound condition, whether internal controls are adequate, and whether the board of directors should take action to address noted issues or problems. The bank's bylaws may also require that directors or a directors' committee participates in the directors' examination at least to appraise the bank's policies and procedures and to review the directors' examination report with the auditors.

Effective directors' examinations normally focus on major risk areas and internal controls and ensure that all areas are adequately covered on a regular

or rotational basis. They should substantially test financial integrity and normally include account reconcilement; asset verification; completion of internal control questionnaires; quality assessment of loans and investments; verification of some or all call report data; review of management information systems; and checks for compliance with laws, regulations, and internal policies. Directors' examinations should include a review of major bank acquisitions and new products and services. These reviews will help ensure that management is following acceptable bank policies and procedures and has instituted sound internal controls.

Independent parties selected by the board to perform directors' examinations should have sufficient knowledge and understanding of banking and understand the bank's business lines. They also should know how to apply accounting and auditing principles and be familiar with the bank's information systems and technology.

## Audit Opinions

An IPA's standard report consists of three paragraphs. The first paragraph identifies the financial statements and differentiates management's responsibilities from those of the auditor. The second, or scope, paragraph describes the nature of the audit and explicitly acknowledges that an audit provides reasonable assurance about whether the financial statements are free of material misstatement. The third paragraph expresses the IPA's opinion.

There are four types of opinions: unqualified, qualified, adverse, and a disclaimer of opinion.[11] An IPA issues an **unqualified opinion** when financial statements present fairly, in all material respects, the financial position, results of operations (i.e., earnings), and cash flows of the entity in conformity with GAAP. Certain circumstances, while not affecting the IPA's unqualified opinion on the financial statements, may require that the auditor add an explanatory paragraph to the report. These circumstances include, but are not limited to, (1) the auditor basing an opinion in part on the report of another auditor and (2) accounting principles changing materially between reporting periods.

[11] For specific standards governing how an IPA derives an audit opinion, examiners and bankers should refer to SAS 58, "Reports on Audited Financial Statements," in the AICPA *Professional Standards*. The AICPA's *Audit and Accounting Guide, Banks and Savings Institutions* provides additional information on audit opinions.

IPAs use a **qualified opinion** when the financial statements present fairly the condition of the bank except in the matters pertinent to the qualification. IPAs use such an opinion when (1) a lack of information or restrictions placed upon the audit prevent them from expressing an unqualified opinion or (2) the financial statements contain a material departure from GAAP.

IPAs use an **adverse opinion** when the matter taken exception to is so substantive that the financial statements do not present fairly the financial condition of the bank. This opinion also covers financial statements that do not conform to GAAP.

IPAs issue a **disclaimer of opinion** when bank management or circumstances restrict in a material way the scope of the auditors' examination.

***When IPAs issue a qualified opinion, adverse opinion, or disclaimer of opinion, they should set forth in the report all material reasons for issuing that particular opinion. Examiners should assess the seriousness of issues raised, corrective actions by the board or management, and how much, if any, validation/testing they should perform. Examiners should also promptly advise the OCC supervisory office of any adverse or disclaimer of opinion encountered.***

## Special Situations

**New national banks.** As a condition of preliminary approval of a newly chartered national bank, the OCC and the FDIC normally require banks to have an annual independent external audit for a period of three years after they open. The first audit should occur no later than 12 months after the bank opens for business. The audit must be of sufficient scope to enable the auditor to render an opinion on the financial statements of the bank or consolidated holding company.

The OCC may grant exemptions from this external audit requirement to a new bank subsidiary of a bank holding company (BHC) when:

- The new bank's financial statements are included in the audited consolidated financial statements of the parent BHC;

- The sponsoring BHC is an existing holding company that has operated for three years or more under Federal Reserve Bank supervision and does not have any institutions subject to special supervisory concerns; and

- Adequate internal audit coverage will be maintained at the bank level. At a minimum, the internal audit program must evaluate the quality of internal controls, including the reliability of financial information, safeguarding of assets, and the detection of errors and irregularities.

The OCC and the FDIC will coordinate determinations about external audit exemptions consistent with the "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," which focuses on banks under $500 million in total assets. If an exemption is granted, the OCC will include that determination in its preliminary conditional approval letter. If any of the requirements listed above are not met during the first three years of the bank's operation, the OCC may withdraw the exemption at its discretion.

The OCC may also waive the external audit requirements for a new bank sponsored by an independent organizing group that is experienced in banking. A group is experienced in banking if a majority of its members have three or more years of recent (the time since such experience should not exceed six months) and significant involvement in policy-making as directors or executive officers in federally insured institutions that the OCC finds have performed satisfactorily. This category may include "chain banking groups." The group must be able to demonstrate that the benefits generally associated with an external audit can be provided substantially by internal expertise or other outside sources.

In most cases, a bank owned by a nonbank holding company does not qualify for an external audit exemption.

For more information, bank directors and management should contact the OCC's licensing division staff in the appropriate district office.

**Institutions presenting supervisory concern.** Sometimes weaknesses in internal controls or management information systems adversely affect financial reporting or contribute to a material deterioration in a bank's safety and soundness. When this happens, the OCC may require the bank to engage independent external auditors and provide the supervisory office copies of

audit reports, including management letters, and to notify the bank's supervisory office prior to any meetings with external auditors.

**Holding company subsidiaries.** When a national bank is owned by a holding company, it may be appropriate for the OCC to address the scope of the bank's external auditing program in the context of the bank's relationship to the consolidated group. If the group's consolidated financial statements are audited, the OCC generally will not require the subsidiary bank to undergo separate financial statement audits. In some cases, however, a subsidiary bank may have activities involving significant risks that are not covered under the procedural scope of the holding company's consolidated audit. In such cases, the bank's directors should consider strengthening internal auditing procedures or implementing an appropriate alternative external auditing program to cover those activities.

External auditing performed for banks not subject to 12 CFR 363 might pertain only to the consolidated financial statements of a holding company. In those circumstances, the examiner should ask the external auditor to describe the audit procedures used to test transactions from subsidiary banks' balance sheets and income statements. If the examiner believes transaction testing may not have been sufficiently extensive, he or she should discuss the matter with the bank and its external auditor.

## Independence

IPAs are subject to the professional standards adopted by their national or state accounting societies or the state agency issuing their licenses. Traditionally, these standards have defined independence as the ability to act with integrity and objectivity. Rule 101 of the *Code of Professional Conduct*[12] adopted by the AICPA states, in part:

> When an IPA expresses an opinion on financial statements, not only the fact, but also the appearance, of integrity and objectivity is of particular importance. For this reason, the profession has adopted rules to prohibit the expression of such an opinion when relationships exist which might pose such a threat to integrity and objectivity as to exceed the strength of

[12] For details regarding AICPA Rule 101 and its interpretations, please refer to the AICPA's Web site (www.aicpa.org).

countervailing forces and restraints. These relationships fall into two general categories: (a) certain financial relationships with clients, and (b) relationships in which the IPA is virtually part of management or an employee under management's control.

FFIEC banking agencies and the SEC require that all public accounting firms that practice in banks or thrifts be independent. Such firms can neither have, nor commit to acquire, a direct financial interest or any material indirect financial interest in the bank or company they are auditing, nor can they be connected as an organizer, underwriter, voting trustee, director, officer, or employee with such a bank or company.[13]

The Independence Standards Board[14] has issued a conflict-of-interest standard (Independence Standard No. 1) that applies to IPAs who conduct external bank audits subject to SEC requirements. The standard requires auditors to disclose, in writing, all relationships with the bank and its related entities that could affect the auditor's objectivity. The auditor's disclosure must also confirm that it is independent in accordance with SEC requirements. Lastly, the auditor must also discuss his or her independence with the bank's audit committee.

The OCC encourages examiners and bankers to consult the AICPA's *Professional Standards* and *Audit and Accounting Guide, Banks and Savings Institutions* for more detail on specific standards or guidance concerning the independence, competence, and objectivity of IPAs.

## Competence

IPAs are required to perform their audits in accordance with GAAS. There are three categories of GAAS standards: general standards, standards of fieldwork, and standards of reporting.[15]

---

[13] The SEC requirements are outlined in 17 CFR 210.2-01 (SEC Regulation S-X), which can be found in appendix A. The SEC requirements are mirrored in 12 CFR 363.

[14] The Independence Standards Board is a private-sector body that establishes independence standards for auditors of public companies. Bankers and examiners should consider this board 's standards when evaluating independence of public accountants.

[15] Refer to SAS 1, "Codification of Auditing Standards and Procedures" of the AICPA *Professional Standards* for specific details.

**General standards** require that an auditor be proficient, having had adequate training in auditing and accounting. The auditor must also be independent in attitude in all matters relating to the assignment. Audits must be conducted using due professional care in the performance of the audit and the preparation of the report. CPAs must have basic education in accounting and auditing that is a prerequisite to taking the uniform CPA examination. Most states have made continuing education a requirement for renewing a CPA license. The AICPA also has continuing education requirements for its members.

**Fieldwork standards** require the auditor to adequately plan the audit and to properly supervise any assistants. The auditor must have sufficient understanding about the bank's internal control structure to plan the audit and to determine the nature, timing, and extent of testing to be performed. The scope of the audit must be sufficient to allow the auditor to obtain enough information through inspection, observation, inquiries, and confirmations to draw a reasonable opinion regarding the financial statements under audit.

**Reporting standards** require the auditor to state whether the financial statements are presented according to GAAP and to identify circumstances in which GAAP has not consistently been followed. The auditor must ensure that the financial statements or the audit report provide adequate disclosures of material items. The report must express an opinion regarding the financial statements taken as a whole or to state that an opinion cannot be expressed. If an overall opinion cannot be expressed, the auditor must state the reasons. The report must give a clear indication of the auditor's work and the degree of responsibility the auditor is taking when his or her name is associated with the financial statements.

## 12 CFR 363 Reports

12 CFR 363[16] and its appendix impose the following auditing, reporting, and audit committee requirements on national banks with $500 million or more in total assets:

- An IPA must audit financial statements.

[16] More detailed information relating to 12 CFR 363 requirements is provided in appendix A.

- Banks must file an annual report and certain other reports with the FDIC and the appropriate OCC supervisory office.

- Banks must have an independent audit committee composed entirely of outside directors.

- The audit committees of national banks with total assets of $3 billion or more must meet more stringent criteria.

- IPAs are subject to reporting, attestation, and examination requirements regarding a bank's internal control structure relating to its financial reporting procedures.

- IPAs must be enrolled in a peer review program and must file a copy of the accounting firm's peer review report with the FDIC.

- IPAs must make the work papers, policies, and procedures from their audits available to OCC examiners for review upon request.

## Other Audits

### Information System/Technology Audits

There are no specific statutory requirements for information system or technology (IS) audits. However, national banks and their service providers are expected to conduct independent assessments of risk exposures and internal controls associated with the acquisition, implementation, and use of information technology. These assessments can be performed by the bank's own internal or external auditor, a servicer's internal auditor, a third party, or any combination of these.

IS audits have two primary goals:

- Verifying the adequacy of technology risk controls.
- Validating the accuracy of automated information.

IS audits should address the risk exposures in information technology throughout the institution and at its service provider(s). The audits should cover such areas as user and data center support and delivery, local and wide

area networks, telecommunications, information security, electronic data interchange, development and acquisition, and contingency planning, as applicable.

The audit usually validates the accuracy of automated information during departmental audits. It involves such activities as transaction testing, reconciling input with output, and balancing subsidiary records to general ledger control totals. These validation procedures can be performed either "around the computer" using source documents and automated reports or "through the computer" by using independent audit software to independently test the production processing environment.

IS audits must cover the processing of transactions by servicing organizations. They usually do so in special audit reports produced in compliance with AICPA SAS 70, "Reports on the Processing of Transactions by Servicing Organizations." An SAS report establishes whether policies and procedures are suitably designed to achieve control objectives, were in effect as of a specific date, and were working well enough to reasonably ensure that control objectives were achieved. Bankers and examiners should not rely solely on SAS 70 reports when assessing the adequacy of audit.

Under the Uniform Rating System for Information Technology (URSIT), part of the evaluation of a bank's information technology system includes an assessment of the IS audit program. Examiners will base their assessment on the same factors used to assess other audits. Examiners and bankers should refer to OCC Bulletin 99-3, "Uniform Rating System for Information Technology" for additional information on assigning a rating for IS audits.[17]

## Fiduciary Audits

The audit requirements for national bank fiduciary activities are set forth in 12 CFR 9, Fiduciary Activities of National Banks. The regulation generally requires national banks with fiduciary powers to perform a suitable audit of all significant fiduciary activities during each calendar year. The board of directors' minutes must note the audit results, including significant actions the bank has taken as a result of the fiduciary audit.

[17] For more information on IS audits, examiners and bankers can refer to the FFIEC's "Information Systems Examination Handbook." It has examination procedures specifically for IS audits.

The OCC and 12 CFR 9 do not define a "suitable audit" or establish minimum audit standards for fiduciary audits. The scope and coverage of fiduciary audits is left to the discretion of the board of directors. The board should base those audits on an appropriate assessment of fiduciary business risk and internal control systems.

In lieu of performing annual audits, 12 CFR 9.9(b) permits national banks to adopt a system of continuous audits. In a continuous audit system, internal or external auditors review each significant fiduciary activity discretely (activity by activity). The audit intervals should be commensurate with the nature and risk of fiduciary activities. Thus, certain fiduciary activities might receive audits at intervals of more or less than one year, as appropriate. At least once during each calendar year, the board of directors' minutes must note the results of all discrete audits performed since the last audit report, including significant actions taken as a result of the audits.

In addition to meeting the audit standards described above, the auditor may need to perform or participate in audits and issue audit reports relating to specific fiduciary activities. The auditors may also rely to some degree on audits of services performed by outside organizations for the subject bank. Activities that may require separate audit attention and reports include:

- Annual study and evaluation of internal accounting control reports of nonexempt registered transfer agents required by 17 CFR 240.17Ad-13.

- Annual audits of collective investment funds in accordance with 12 CFR 9.18(b)(6).

- Annual financial statements based on audits of proprietary mutual funds in compliance with applicable securities laws.

- Internal control audits covering the bank's performance of certain fiduciary services for other organizations.

- External control audits, using criteria in AICPA SAS 70, covering the fiduciary bank's functions that rely on the services of an outside organization.

The board of directors' audit committee (or fiduciary audit committee) typically directs fiduciary audits and reviews the audit work and reports for

each audit process. The committee should determine whether the reports are adequate and can be relied upon.

Examiners will base their assessment of the fiduciary audit on the same factors used to assess other audits. The examination procedures in the "Community Bank Fiduciary Activities Supervision" booklet of the *Comptroller's Handbook* help examiners to determine whether a community bank complies with 12 CFR 9 and whether its fiduciary audit is adequate.

Under the Uniform Interagency Trust Rating System (UITRS), the fiduciary activities of national banks are assigned a composite rating for five areas. One of those areas is operations, controls, and audits. For this area to be considered adequate, audit coverage must ensure the integrity of the financial records, the sufficiency of internal controls, and the adequacy of the compliance process.[18]

## Consumer Compliance Audits

The audit of consumer compliance, as part of a bank's compliance management system, enables the board of directors and senior management to monitor the effectiveness of a bank's compliance program. The formality and structure of a compliance audit depends on a bank's size, the nature of its activities, and its risk profile. In some large banks, for example, compliance audits are done on a systemic basis or on a business-by-business basis as appropriate to the structure of the bank. The function may be under the auspices of a bank's internal audit department, or it may be a direct responsibility of a bank's compliance division.

The audit tests compliance with consumer protection laws and regulations as well as staff adherence to established policies and procedures. The audit should address all products and services offered by a bank, all aspects of applicable operations, and all departments and branch locations. Examiners evaluate the compliance audit using the same criteria they use for any other type of audit.

The Uniform Interagency Consumer Compliance Rating System takes into consideration a bank's compliance audit functions. When assigning a

[18] OCC Bulletin 98-46, "Uniform Interagency Trust Rating System," provides further information on assigning trust ratings.

consumer compliance rating, examiners must consider the adequacy of operating systems, including internal procedures, controls, and audit activities that the bank uses to ensure compliance with applicable consumer laws, rules, and regulations.[19]

[19] Additional detail on how examiners assess compliance audit functions is included in the "Compliance Management Systems" and "Community Bank Consumer Compliance" booklets of the *Comptroller's Handbook for Compliance*.

# Examination Procedures

These procedures are intended to help examiners determine the quality and reliability of the bank's policies, procedures, personnel, and controls with respect to internal and external audits. The procedures are not meant to be performed strictly in the order presented, but should be fit to the bank's or examination's particular circumstances. The review of internal and external audit functions should be closely coordinated with the reviews of examiners responsible for other areas of the bank (e.g., credit, capital markets, compliance, fiduciary, and information systems). Such coordination can reduce burden on the bank, prevent duplication of examination efforts, and be an effective crosscheck of compliance and process integrity.

**These examination procedures supplement the minimum core assessment audit objectives in the "Community Bank Supervision" and "Large Bank Supervision" booklets. Examiners should begin their audit review with the minimum objectives and steps from those booklets. The examiners' assessment of risk, the supervisory strategy objectives, and any examination scope memorandum should determine which of this booklet's procedural and validation steps to perform to meet examination objectives. Seldom will every objective/step of this booklet's procedures be required to satisfy examination objectives.**

## Planning the Audit Review

Objective: Determine the scope and objectives of the examination of the internal and external audit functions.

1. Obtain and review the following documents to identify any previous problems that require follow-up:

   - ☐ Previous Report of Examination and key supervisory information (e.g., strategy, analyses, other significant events) in OCC databases.
   - ☐ EIC's scope memorandum, if applicable.
   - ☐ OCC audit summary memos and working papers from the previous examination.
   - ☐ Internal and external audit reports, including audit reports that the auditors may have participated in or relied on to any extent, such as

AICPA SAS 70 reports ("Reports on the Processing of Transactions by Servicing Organizations").

- ☐ Audit policies and manuals, including those applicable to sampling plans, risk-based auditing, or outsourcing of internal audit functions.
- ☐ Minutes of the audit committee(s), including the fiduciary audit committee, if applicable, and applicable board of directors' minutes since the last examination.
- ☐ Listing of members of the audit committee(s), including those on the fiduciary audit committee, if applicable, and the date of each member's appointment to committee.
- ☐ Audit plans and scopes, including any external audit or internal audit outsourcing engagement letters.
- ☐ The institution's annual reports.
- ☐ Correspondence memorandum.

2. Identify during early discussion with management and review of the most recent internal and external audit reports:

   - How management supervises audit activities.
   - Any significant changes in business strategy or activities that could affect the audit function.
   - Any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities.
   - Any other internal or external factors that could affect the audit function.

3. Obtain a list of outstanding audit items and compare the list with audit reports to ascertain completeness. Determine whether all significant deficiencies noted in the audit reports have been corrected and, if not, determine why corrective action has not been initiated. Make those determinations by:

   - Distributing to each examiner responsible for an examination area a copy of the area's audit report or a list of significant audit deficiencies for that area.

   - Requesting that the examiner prepare and return a memorandum stating whether the board or management has addressed the audit deficiencies and whether their actions were adequate.

4. Identify internal audit work programs, including those from any outsourced internal audit activities and directors' examination, from which to select a reasonable sample of internal audit work papers for validation purposes. Coordinate validation efforts with the examiners reviewing functional or specialty areas (e.g., credit, capital markets, compliance, information systems, and fiduciary) and:

   - Provide the examiner(s) with the audit program(s) and audit report(s) for the specific area(s) to be tested.

   - Request that applicable internal audit work papers be made available to the examiner(s) for review.

   **Note:** A sample of internal audit work papers will be reviewed during every examination cycle. The sample should be sufficient to provide a basis to validate the scope and quality of the internal audit program. The sample should represent a cross-section of bank activities, functions, and internally assigned audit ratings, with a bias toward high-risk and rapid growth areas, technology audits, and products/activities new to the bank.

# Quality of Audit

**Conclusion: The quality of audit management is (strong, satisfactory, weak).**

## Internal Audit

### Statutory Requirements

Conclusion: The board of directors' and management's compliance with internal audit-related laws and regulations is (strong, satisfactory, weak).

Objective: Using the following steps and other findings from the review of the bank's internal audit function, determine compliance with the following statutory requirements for internal auditing and reporting.

**12 CFR 30, Safety and Soundness Standards**

1. Determine whether the bank has an internal audit system that is appropriate to its size and the nature and scope of its activities. Also determine whether the system complies with 12 CFR 30, Safety and Soundness Standards, Appendix A, "Operational and Managerial Standards," in providing for:

   - Adequate monitoring of internal control systems.
   - Independence and objectivity.
   - Qualified persons.
   - Adequate testing and review of information systems.
   - Adequate documentation of tests, findings, and corrective actions.
   - Verification and review of management actions addressing material weaknesses.
   - Board of directors or audit committee review of the internal audit systems' effectiveness.

## 12 CFR 9, Fiduciary Activities of National Banks

**Note:** Examiners should perform the following steps if they are not being performed as part of an asset management examination or review.

1. Determine whether the OCC has granted the institution the power to act in a fiduciary capacity (12 CFR 9.3).

   If so, proceed with steps 2 through 4 by reviewing previously requested materials.

2. Verify whether a suitable audit of the bank=s significant fiduciary activities is conducted, including any audit reports that the internal auditors may have participated in or relied on to any extent, such as AICPA SAS 70 ("Reports on the Processing of Transactions by Servicing Organizations") audits by external auditors:

   - At least once during a calendar year (12 CFR 9.9(a)), or under a continuous audit system in conformance with 12 CFR 9.9(b).

   - Under the direction of the bank's fiduciary audit committee (12 CFR 9.9(a) and (b)).

   - With the results of the audit, including significant actions taken as a result of the audit, noted in the minutes of the board of directors (12 CFR 9.9(a)). Alternatively, under a continuous fiduciary audit program, results and actions of all discrete audits completed should be noted in board minutes at least once during each calendar year (12 CFR 9.9(b)).

3. Determine whether the institution has a fiduciary audit committee structured along the following lines (to comply with applicable provisions of 12 CFR 9.9(c)):

   - Members of the audit committee do not include officers who participate significantly in the administration of the bank's fiduciary activities (12 CFR 9.9(c)(1)).

- A majority of committee members are not also members of other committees delegated power to manage and control the bank's fiduciary activities (12 CFR 9.9(c)(2)).

4. If the bank has established collective investment funds, obtain the most recent audit of each fund and give it to the examiner responsible for reviewing that activity (12 CFR 9.18(b)(6)(l)).

## Policy

Conclusion: The board has established (strong, satisfactory, weak) policies governing the internal audit function.

Objective: Determine the adequacy of written policies relative to the internal audit program, including directors' examinations.

1. If not previously provided, obtain copies of:

   - ☐ Audit charter or mission statement, if any.
   - ☐ Internal audit manuals and policies.

2. Review policies and manuals pertaining to the bank=s internal audit function, including, as applicable, those related to risk-based audits, outsourcing of activities, and directors' examinations. Consider whether written policies:

   - Are adequately reviewed and approved by the board of directors or its audit committee annually.
   - Properly reflect authorities and responsibilities established by the audit charter or mission statement.
   - Establish proper scope and frequency for an audit review. Consider:
     - Statutory requirements and regulatory guidelines.
     - Purpose and objectives of audits.
     - Control and risk assessments.
     - Audit cycles.
     - Reporting relationships and requirements.

**Note:** Banks using traditional auditing typically will have audit cycles of 12 to 18 months. However, banks using risk-based auditing or internal risk assessments generally have audit cycles of varying lengths based on the level of risk in an activity. See risk-based auditing objective under "Processes" for details.

- Establish adequate guidelines for human resources involved in the audit function. Consider:

  – Organization and independence of the audit department.
  – Responsibilities of audit staff.
  – Job standards and qualifications.
  – Training and development.
  – Performance evaluations.

## Personnel

Conclusion: The board of directors has established a (strong, satisfactory, weak) internal audit function with respect to the competence and independence of those who provide the internal audit function and those who supervise internal audit activities to ensure their adequacy.

Objective: Evaluate the competence of those who manage and perform internal audit functions, whether or not they are bank employees.

1. Obtain the following:

   ☐ Resumes of the internal auditor/manager, new internal audit staff, or those recently promoted to senior levels.
   ☐ Job descriptions for various audit positions.
   ☐ As deemed appropriate, performance evaluations of the audit manager and selected audit staff.

2. Assess the educational and professional experience of the internal auditor and staff by reviewing resumes and noting:

   - The level of education attained.

- Significant work experience, especially in the bank auditing arena, including specialized areas such as capital markets, information systems, fiduciary activities, and subsidiary activities.

- Any certification as a certified bank auditor, certified internal auditor, certified information systems auditor, or certified public accountant.

- Membership in professional associations.

3. Review job descriptions and discuss with the audit manager:

   - Educational and experience requirements for various audit positions, including those for specialized areas.

   - Programs of continuing education and professional development, including in banking and auditing technology and specialized areas.

   - Supervision of the auditors.

4. If deemed appropriate, review performance evaluations of the audit manager and audit staff. Determine how identified strengths and weaknesses in supervisory, technical, or interpersonal skills or abilities affect the quality of the internal audit function.

5. Assess audit personnel turnover and vacancies, focusing on the reasons for turnover/vacancies and their effect on the internal auditing function.

6. Evaluate the ability of the audit manager and staff to communicate and interact with other institution personnel.

Objective: Evaluate board oversight and independence of the internal audit function:

1. Determine whether there are any operational duties assigned to the auditor that are incompatible with the internal audit function.

2. Ascertain whether there is any auditor relationships, such as family ties with other bank employees, which are incompatible with the internal audit function.

3. Determine whether there are any restrictions placed on the internal audit program, including scheduling or budgetary restraints imposed by management.

4. Ensure that the board or its audit committee reviews or approves the budget, salary, and performance evaluation of the internal audit manager.

## Processes

Conclusion: The adequacy and reliability of the internal auditors' work shows that management and the board have established (strong, satisfactory, weak) internal audit processes.

Objective: Determine the adequacy, effectiveness, and quality of the bank's directors' examination.

1. Determine whether the bank's bylaws require the board of directors to have independent parties periodically examine and report on the bank's affairs (i.e., directors' examination).

2. Determine whether directors, or a committee of directors, participate in the directors' examination at least to appraise the bank's policies and procedures and to review the directors' examination report with the auditors.

3. Determine whether the directors' examination focuses on major risk areas and internal controls and encompasses:

   - Substantively testing financial integrity.
   - Reconciling accounts.
   - Verifying assets.
   - Completing internal control questionnaires.
   - Assessing the quality of loans and investments.

- Verifying some or all call report data.
- Reviewing management information systems.
- Confirming the bank's compliance with laws, regulations, and internal policies.
- Reviewing acquisition and/or merger activities.
- Reviewing new products and services.

4. Review the directors' examination report findings and determine whether it addresses:

   - The bank's soundness.
   - The adequacy of internal controls.
   - The actions the board should take to address noted issues or problems.

5. Determine whether the board ensured that independent parties selected to perform the directors' examination possessed:

   - Sufficient knowledge and understanding of banking.
   - Knowledge and understanding of the bank's operations and activities.
   - Ability to apply accounting and auditing principles.
   - Familiarity with the bank's information systems and technology.

Objective: Determine whether the internal risk analysis processes are adequate for the bank's size, the nature and extent of its banking activities, and its risk profile.

1. Determine whether the bank has appropriate standards and processes for risk-based auditing and internal risk assessments. Such standards and processes should:

   - Identify businesses, product lines, services, or functions and the activities within those that should be audited.

   - Develop risk profiles that identify and define the risk and control factors to assess and the risk management and control structures for each business, product line, service, or function.

- Establish the process for grading or assessing risk factors for business units, departments, products, or functions, including time frames.

- Describe how the process is used to set audit plans, resource allocations, scopes of audits, and audit cycle frequency.

- Implement audit plans through planning, execution, reporting, and follow-up.

- Establish minimum documentation requirements to support scoring or assessment decisions and draw conclusions.

- Define when overrides of risk-based scores or assessments are acceptable or necessary, including which level of authority approves overrides.

- Provide for confirming the system regularly, i.e., annually or whenever significant changes occur within a department or function.

2. Select a sample of auditable units (i.e., business lines, product lines, services, or function) and determine the reasonableness of the internal risk analysis decision, including application of any risk models used.

3. Determine whether audit cycle frequencies are reasonable and are being met.

   **Note:** In a risk-based audit system, banks set audit cycles based on risk scores/assessments. Customarily, banks may set audit cycles at 12 months or less for high-risk areas, 24 months or less for moderate-risk areas, and more than 24 months for low-risk areas. Individual circumstances at each bank will determine how it establishes audit cycle lengths.

4. If audit management has overridden risk-based audit schedules, discuss justifications with the audit manager.

5. If applicable, determine the quality and effectiveness of internal audit's ongoing monitoring of the bank's business operations.

Objective: Determine the adequacy and the reliability of work performed by the internal auditors.

1. If not previously provided, obtain copies of or access to:

   - ☐ Internal audit reports.
   - ☐ Internal audit work papers.

2. Using internal audit work programs previously identified in "Planning the Audit Review," obtain or request access to audit work papers to complete the remaining objectives and steps. Consider having examiners responsible for other areas of the bank (e.g., credit, capital markets, compliance, information systems, fiduciary) review internal audit work programs and work papers associated with those activities.

   **Note:** In most situations, reviewing the **work papers** that document the procedures and testing performed by the internal auditor should be sufficient to substantiate conclusions about the quality and reliability of the internal auditing function. Findings from the work paper reviews will help determine whether further verification or testing is warranted.

   If, in achieving the following objectives and performing the following steps, concerns remain about the adequacy of internal audit, the soundness of internal controls, or the integrity of financial controls, the examiner should perform appropriate **verification procedures**, including completing **internal control questionnaires (ICQs)** as needed.[20]

   For less problematic situations, the examiner may require the bank to expand its audit program to include the areas of weakness or deficiency. However, this alternative will be used only if management has demonstrated a capacity and willingness to address regulatory problems, if there are no concerns about management's integrity, and if management has initiated timely corrective action in the past. Use of this alternative must result in timely resolution of each identified supervisory problem. If examiners use this alternative, supervisory

[20] Verification procedures are required in certain situations. See the "Supervisory Process and Validation" section of this booklet for specific details.

follow-up will include a review of audit work papers in areas where the bank audit was expanded.

3. Review the bank's internal audit program for completeness and compliance with prior board or audit committee approval.

4. Analyze the internal auditor's evaluation of departmental internal controls and compare it with the control evaluations done by OCC examiners.

5. Review internal audit reports to determine whether they are adequate and prepared in accordance with established audit policy. Consider the reports':

   - Distribution

     – To division heads/senior management responsible for taking action.
     – To internal audit staff, as appropriate.
     – To board of directors or its audit committee.

   - Time frames

     – Audit findings discussed with appropriate parties (i.e., division personnel or senior management) after completion of audit work.
     – Responses obtained from appropriate parties after discussion of audit findings.
     – Final report issued after discussion of audit findings and receipt of responses.

   - Content

     – Executive summary or opening paragraph.
     – Statements on the audit's purpose, objectives, and scope.
     – Findings, recommendations, and other comments.
     – Management commitments.
     – Opinion or grading summary.

- Follow-up

  - Written responses from audited parties to division or senior management and the internal auditor.
  - Auditor's review and discussion of corrective action efforts or results with appropriate parties.
  - A re-audit, if performed.

6. Review the most recent audit plan and determine whether adequate coverage and internal risk assessment is provided for all areas of bank operations (for example, cash, loan controls, conflicts of interest, off-balance-sheet activities, negotiable instruments, interoffice clearing accounts, due from banks, employee accounts, overdrafts, and payments against uncollected funds.)

7. If the bank uses sampling in asset verification, transactional testing, administrative audits, etc., determine whether the audit work program addresses:

   - Objectives of testing.
   - Procedures to meet objectives.
   - Populations subject to sampling.
   - Method of sampling (i.e., statistical or judgmental).
   - Selecting a representative sample sufficient to support conclusions.
   - Evaluation of results and documentation of conclusions.

   **Note:** Examiners can refer to the "Sampling Methodologies" booklet for detailed guidance about statistical and judgmental sampling.

8. Evaluate the scope of the internal auditor's work as it relates to the bank=s size, the nature and extent of banking activities, and the bank's risk profile.

   - Do the work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the reports? Consider:

     - Verification of account balances (reconciliation, confirmation, and physical count).

- Review/test of income and expense accounts, accruals, gains/losses, including computations.
- Transaction testing and testing the value or pricing of assets (i.e., investments, collateral).
- Physical inspection of legal and supporting documentation, including validation of authorities granted (i.e., making/approving loans, signing official bank documents, etc.).
- Review of information system data controls.
- Review and evaluation of policies, procedures, and internal controls.
- Checks of compliance with laws/regulations.
- Checks of adherence to bank policy.

• Is the scope of the internal audit procedures adequate and properly documented? Consider:

- Audit planning memoranda.
- Checklists.
- Internal control questionnaires.
- Control and risk assessments.
- Previous audit reports, responses, and follow-up.
- Procedures performed (general and specific).
- Testing conducted.

Objective: If the internal audit function, or any portion of it, is outsourced to outside vendors, determine the effectiveness of and reliance to be placed on the outsourced internal auditing.

1. Obtain copies of:

   ☐ Outsourcing contracts or engagement letters.
   ☐ Outsourced internal audit reports.
   ☐ Policies on outsourced audit, if any.

2. Review the outsourcing contracts/engagement letters and policies to determine whether they adequately:

   • Set the scope and frequency of work to be performed by the outside vendor.

- Set the manner and frequency of reporting to the bank=s audit manager, senior management, and audit committee or board of directors about the status of work.

- Establish protocol for changing terms of the service contract, especially for expansion of audit work if significant issues are found.

- State that internal audit reports are the property of the institution, that the vendor will provide copies of related work papers the bank deems necessary, and that authorized employees of the bank will have reasonable and timely access to work papers prepared by the outside vendor.

- Identify the locations of outsourced internal audit reports and related work papers.

- Grant OCC examiners immediate and full access to outsourced internal audit reports and related work papers.

- Prescribe an alternative dispute resolution process for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.

- State that outside vendors, if subject to AICPA independence guidance, will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee of the institution.

3. Determine whether the outsourcing arrangement maintains or improves the quality of the internal audit function and the institution's internal controls.

   - Review the performance and contractual criteria for the vendors and any internal evaluations of the vendor.

   - Review outsourced internal audit reports and a sample of audit work papers. Determine whether they are adequate and prepared in accordance with the audit program and the outsourcing agreement.

- Determine whether work papers disclose that specific program steps, calculations, or other evidence support the procedures and conclusions set forth in the outsourced reports.

- Determine whether the scope of the outsourced internal audit procedures is adequate. Consider:

  - Procedures performed.
  - Testing conducted.
  - Approval of the internal audit manager.

4. Determine whether key employees of the institution and the vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the outside vendor are to be addressed. Consider whether:

   - Results of outsourced work are first reported to the bank's audit manager or internal auditor or other individual responsible for overseeing the bank's internal audit function.

   - The internal auditor or audit manager, individually or jointly with the vendor, reports findings to the board or its audit committee and senior management.

5. Determine whether the scope of outsourced audit work is revised appropriately when the institution's environment, activities, risk exposures, or systems change significantly.

6. Determine whether the directors have ensured that any outsourced internal audit function is effectively managed by the institution.

7. Determine whether the directors have performed sufficient due diligence to satisfy themselves of the vendor's competence before entering the outsourcing arrangement.

8. Determine whether the institution has adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.

9. If the vendor is a CPA who does not also perform the external audit, determine whether any potential conflicts of interest have been properly addressed (AICPA Ruling 102-2, Conflicts of Interest).

10. If the vendor also performs the bank's external audit, determine whether independence is compromised (AICPA Rule 101, Interpretation 101-13, and rules 103, 104, and 105).

11. If, in performing the preceding steps, there is sufficient reason to question the independence, objectivity, or competence of the vendor, discuss the situation with OCC district management, the Chief Accountant's office, and/or the Chief Counsel's department.

    - If appropriate, request through the bank that additional work papers be made available or meet with the vendor to discuss the concerns.

12. If the OCC determines that it cannot rely on the vendor's work, discuss that assessment with the board, bank management, and the affected party before finalizing the report of examination.

## Controls

Conclusion: The board and management (have/have not) established effective control systems for internal audits.

Objective: Determine whether the board and management have instituted controls that are appropriate for the type and level of risks arising from the internal audit function.

1. Determine whether the board has established an audit program that employs:

    - An audit charter or mission statement that sets forth the audit department's purpose, objectives, organization, authority, and responsibilities.

    - An audit plan that addresses goals, schedules, staffing budget, reporting, and, if applicable, financial budgets.

- A policies and procedures manual for audit work programs and, if applicable, risk-based auditing/risk assessments and outsourcing of internal audit work.

- A program for training audit staff, including orientation and in-house and external training opportunities.

- A quality assurance program, performed by internal or external parties, to evaluate the operations of the internal audit department.

2. Review board or audit committee minutes, or summaries thereof, and determine whether:

   - The audit program and schedule have been formally approved by the board of directors or its audit committee.

   - Audit reports are monitored to determine whether approved programs and schedules are followed.

   - The audit program and schedule are periodically reviewed and updated by the internal audit department.

   - Progress has been made toward completing the audit program or schedule and the board or audit committee has approved significant audit program/schedule changes.

   - Reasonable consideration is given to staffing, compensation, and training requirements.

   - Management does not unduly participate in or dominate the directors' supervision of the internal audit function.

3. Review management's records supporting any assertions concerning the effectiveness of internal controls over financial reporting and compliance with designated laws and regulations.

4. Determine whether management's standards for measuring the adequacy and effectiveness of internal controls over financial reporting are appropriate. Consider:

   - Sources of established standards (e.g., AICPA, OCC, Committee of Sponsoring Organizations of the Treadway Commission [COSO], etc.).
   - Risk analyses or assessments.
   - Control assessments.
   - Audit report findings.

5. Determine whether the internal auditor reports directly to the board or to an appropriate audit committee.

6. Determine whether management takes appropriate and timely action on internal audit findings and recommendations and whether it reports the action to the board of directors or its audit committee.

7. Determine whether the activities of the internal audit function are consistent with the long-range goals of the institution and are responsive to its internal control needs.

8. For banks that have a quality assurance program, evaluate the adequacy and effectiveness of the program by determining whether:

   - Standards and criteria have been established for evaluating the performance of the internal audit function.

   - Quality assurance is conducted by:

     – Continuous supervision by the internal audit manager,
     – Periodic internal reviews by a team or individual from the internal audit staff, or
     – External reviews by qualified persons independent of the bank.

   - Any type of formal report, written or oral, is generated and to whom the report is generated (i.e., internal audit manager, senior management, or board of directors or its audit committee).

   - Quality assurance reviews are conducted regularly.

## External Audit

### Statutory Requirements

Conclusion: The bank's compliance with external-audit-related laws and regulations is (strong, satisfactory, weak).

Objective: If applicable, use the following steps and other findings from the review of the bank's external audit function to determine compliance with the following statutory requirements for external auditing, audit committee, and reporting.

**12 CFR 363, Annual Independent Audits and Reporting Requirements**

1. Determine whether the bank is subject to the auditing, reporting, and audit committee requirements of 12 CFR 363 and its guidelines.

   - Did the bank have total assets at the beginning of its fiscal year of $500 million or more (12 CFR 363.1(a))?

   If so, proceed with steps 2 through 14 by reviewing requested materials and performing other external-audit-related steps.

2. Determine whether the bank is owned by a holding company and relies on holding company audit coverage.

   If so, for banks other than lead banks, determine whether the bank qualifies for, and has invoked, the holding company exception by determining whether:

   - Holding company financial statements are audited on a consolidated basis (12 CFR 363.1(b)(1)).
   - The holding company has services and functions comparable to those required of the bank (12 CFR 363.1(b)(2)(I)).
   - As of the beginning of its fiscal year, the bank had:
     - Total assets of less than $5 billion (12 CFR 363.1(b)(2)(ii)(A)); or

- Total assets of $5 billion or more and a composite CAMELS rating of 1 or 2 (12 CFR 363.1(b)(2)(ii)(B)).

- The OCC or FDIC revoked the exception in 12 CFR 363.1(b)(2) because the bank has total assets of $9 billion or more and the agency determined that exempting the bank would place the deposit insurance fund at significant risk (12 CFR 363.1(b)(3)).

- Any other information about the subject bank in holding company reports is pertinent to its exception.

**Note:** For holding company lead banks, consider performing the following procedures based on holding company records.

3. Determine whether the institution has prepared a management report, as of its most recent fiscal year end, that is signed by its chief executive officer and chief accounting or chief financial officer (12 CFR 363.2(b)).

   The management report should contain:

   - A statement of management's responsibilities for:

     - Preparing the institution's annual financial statements.
     - Establishing and maintaining adequate internal control structures and procedures for financial reporting.
     - Complying with laws and regulations relating to safety and soundness which are designated by the OCC (12 CFR 363.2(b)(1)).

   - Assessments by management of:

     - The effectiveness of internal control structures and procedures as of the end of its fiscal year.
     - The institution's compliance with laws and regulations during the fiscal year (12 CFR 363.2(b)(2)).

4. Determine whether the institution has engaged an independent public accountant (IPA) to audit and report on its financial statements in accordance with generally accepted auditing standards (GAAS) (12 CFR 363.3(a)).

5. Determine whether the IPA, in accordance with generally accepted standards for attestation engagements (GASAE), has examined, attested to, and reported separately on management's assertions concerning internal control structure and procedures for financial reporting (12 CFR 363.3(b)).

6. Determine whether the IPA who performed an audit under 12 CFR 363 has terminated their services.

   If so, verify that the IPA properly notified the OCC and FDIC of such termination (12 CFR 363.3(c)). Such notification should:

   - Be in writing.
   - Be submitted within 15 days of the termination.
   - Set forth the reasons for such termination.

7. Determine whether the bank has selected, changed, or terminated its IPA.

   If so, determine whether the institution has notified the OCC and FDIC (12 CFR 363.4(d)). The notice should:

   - Be in writing
   - Be filed within 15 days of the event.
   - Give reasons for the event.

8. Determine whether the bank has an audit committee structured to comply with 12 CFR 363.5(a).

   - Is the committee made up entirely of outside directors of the bank?

   - Are the members independent of the management of the bank? Consider whether the director:
     - Is, or has been within the preceding year, an officer or employee of the institution or its affiliates.
     - Serves or served as the institution's or its affiliates' consultant, advisor, promoter, underwriter, legal counsel, or trustee.
     - Is a relative of an institution's or its affiliates' officers or employees.

- Holds or controls, or held or controlled within the preceding year, either directly or indirectly, a financial interest of 10% or more in the institution or its affiliates.
- Has outstanding extensions of credit from the institution or its affiliates.

- Do the committee's duties include the following:
  - Performing all duties determined by the institution's board of directors?
  - Reviewing the basis of required reports (363.2(a) and (b) and 363.3(a) and (b)) with management and IPA?
  - Reviewing with management and the IPA the scope of services required by the audit, significant accounting policies, and audit conclusions regarding significant accounting estimates?
  - Reviewing with management and the IPA their assessments of internal control adequacy and resolution of identified material internal control weaknesses and reportable conditions?
  - Reviewing with management and IPA the institution's compliance with laws and regulations?
  - Discussing with management the selection and termination of the IPA and any significant disagreements between the IPA and management?
  - Overseeing the internal audit function?
  - Maintaining minutes and other relevant records of their meetings and decisions?

9. For banks with assets of more than $3 billion, determine whether the audit committee complies with 12 CFR 363.5(b). Confirm that the committee has:

   - At least two members with the following banking or related financial management expertise:

     - Significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters as determined by the board of directors, or

     - Significant experience as an officer or member of the board of directors or audit committee of a financial services company.

- Access to its own counsel at its discretion and without prior approval of the board or management.

- No member who is a large customer of the bank.

**Note:** If a large bank is a subsidiary of a holding company and relies on the audit committee of the holding company to comply with this requirement, the holding company's audit committee shall not include any members who are large customers of the subsidiary bank.

10. Determine whether management has performed its own investigation and review for compliance with designated laws (appendix A to 12 CFR 363, table 1).

    - Has management maintained records of its review?
    - Were the results of the review discussed with the audit committee?

11. Note any exceptions to 12 CFR 363 reporting or audit committee requirements or activities.

12. Determine whether the institution properly filed an annual report in accordance with 12 CFR 363.4(a). Verify that:

    - Two copies each of the annual report were filed with the OCC and FDIC.

    - The report was filed within 90 days after the institution's fiscal year-end.

    - The annual report included:

      – Audited financial statements.
      – Independent public accountant's report on the financial statements.
      – Management's statements and assessments.
      – Independent public accountant's attestation report concerning the institution's internal control structure and procedures for financial reporting.

13. Determine whether the institution's annual report is available for public inspection (12 CFR 363.4(b))

14. Determine whether the institution filed with the OCC and FDIC copies of audit reports and any management letters, qualifications, or other reports (including attestation reports) from the bank's independent public accountant within 15 days of receipt (12 CFR 363.4(c)).

**15 USC 78, Securities Exchange Act of 1934**

1. Determine whether the bank is required to have its financial statements audited by an independent public accountant (15 USC 78m). If the bank has more than $1 million in total assets and 500 shareholders, and its equity securities are registered with the OCC (15 USC 78l(g)(1)), it is required to do so (15 USC 78m(a)(2)).

**Note**: National banks that have their securities registered with the OCC or with the New York Stock Exchange (NYSE), American Stock Exchange (AMEX), or National Association of Securities Dealers, Inc. (NASD) are subject to the following Securities and Exchange Commission (SEC) regulations. These requirements are in addition to requirements imposed by 12 CFR 363.

**17 CFR 210.2-01, Qualifications and independence of independent public accountants (IPAs) engaged to perform services for companies with a class of securities registered pursuant to the Securities Exchange Act of 1934.**

1. Determine whether the bank's IPA is duly registered and in good standing under the laws of the place of his/her residence or principal office.

2. Confirm that, during the IPA's professional engagement to examine the bank's financial statements on which the IPA is reporting or on the date of the report, the IPA, his/her firm, or a member of his/her firm did not have, or was not committed to acquire, any direct financial interest or any material indirect financial interest in the bank.

3. Confirm that, during the IPA's professional engagement to examine the bank's financial statements on which the IPA is reporting, on the date of the report, or during the period covered by the financial statements, the

IPA, his/her firm, or a member of his/her firm was not connected as a promoter, underwriter, voting trustee, director, officer, or employee of the bank.

### 17 CFR 210.10-01, Interim Financial Statements

1. Determine whether the IPA reviewed interim financial statements included in the bank's quarterly 10-Q reports using procedures in SAS 71, "Interim Financial Information."

### 17 CFR 229.306, Audit Committee Report

1. Determine whether the bank's audit committee, as part of proxy and information statements for meetings at which directors are to be elected, made a report stating whether the audit committee:

   - Reviewed and discussed audited financial statements with management.

   - Discussed with the company's IPA the matters required to be discussed by SAS 61, "Communication with Audit Committees."

   - Received the written disclosures and the letter from the IPA (as required by Independence Standards Board Standard No. 1, "Independence Discussions with Audit Committees"), and discussed the IPA's independence with the IPA.

   - After taking the preceding actions, recommended to the board of directors that the audited financial statements be included in the company's annual report.

2. Determine whether the names of each member of the bank's audit committee appear below the above-referenced disclosures. In the absence of an audit committee, the names of the board committee performing the equivalent functions or the names of the entire board must appear.

**17 CFR 240.14a-101, Information Required in a Proxy Statement, Schedule A, Item 7**

1. If the registered bank has an audit committee, determine whether the proxy statement:

   - Provides the information required by 17 CFR 229.306.
   - States whether the board of directors has adopted a written charter for the audit committee.
   - Includes a copy of the written charter, if any, as an appendix to the proxy statement at least once every three years.

2. If the registered bank's securities are listed on the New York Stock Exchange (NYSE) or American Stock Exchange (AMEX) or quoted on National Association of Securities Dealers Automatic Quotation (Nasdaq), determine whether the bank disclosed:

   - Whether audit committee members are independent.
   - If a member is not independent, the nature of the relationship that makes the member not independent and the reasons for the board's determination.

**Note:** For purposes of steps 1 and 2, the NYSE, AMEX, or National Association of Securities Dealers (NASD) definition of independence is used.

3. If the registered bank is not listed on the NYSE or AMEX or quoted on Nasdaq, determine if the bank disclosed whether audit committee members are independent.

## Policy

Conclusion: The board has established (strong, satisfactory, weak) policies governing the external audit function.

Objective: Determine the adequacy of any policies pertaining to the external audit program.

1. Review any policies pertaining to the bank=s external audit function and determine whether they:

   - Are adequately reviewed and approved by the board of directors or its audit committee at least annually.

   - Establish proper scope and frequency for audit reviews. Consider:

     – Statutory requirements and regulatory guidelines.
     – Purpose and objectives of audits or reviews.
     – Type of audit or review performed.
     – Reports issued.

   - Establish adequate guidelines for human resources involved in the audit function. Consider:

     – External auditor qualifications, education, and experience.
     – Involvement of internal audit staff.

2. If a community bank does not have an external auditing program, discuss the circumstances with the board and management. Focus on:

   - Why the board decided not to have an external audit.
   - The benefits of an external auditing program.
   - Whether such benefits are being provided by an alternative means such as internal expertise or other outside sources.

## Personnel

**Note:** Which steps in "Personnel" and "Processes" must be performed depends considerably on whether the auditor is a CPA or not. Other factors to consider are the examiner's familiarity with the external auditor's professional reputation, the extent of any previous validation/testing of the auditor's work, and whether problems or issues arise regarding the auditor's independence, objectivity, and competence.

Conclusion: The board of directors has established a (strong, satisfactory, weak) external audit function with respect to the competence and independence of

those who provide the external audit function and those who supervise the audit activities.

Objective: Evaluate the independence, objectivity, and competence of those who provide the external audit function.

1. Arrange a meeting with knowledgeable officials of the bank to discuss the following:

   - The relationship of the external auditors to the bank and to any director, officer, or employee to determine whether such relationships compromise the auditor's independence.

   - Any significant dealings the external auditors may have or may have had with the bank in the form of stock holdings or borrowings. Review the terms of any such dealings. Any loans to a CPA or his or her firm should be in keeping with the AICPA *Professional Standards*, "Code of Professional Conduct", ET section 101.

   - Whether the external auditor also performs any of the bank's outsourced internal audit work. If so, determine that the auditor's independence is not compromised and is maintained in accordance with rulings 103, 104, and 105 and interpretation 101-13 of the AICPA's Rule of Conduct 101.

   - The professional reputation of the auditors.

2. Determine whether the bank has recently changed external auditors and discuss with appropriate bank management the reasons for such change. Particular attention should be given to disagreements between the external auditor and management about the appropriate accounting principles applicable to specific transactions or matters.

3. Arrange through the bank to meet with non-CPA external auditors, if applicable, to discuss relevant education and experience. Consider the following:

   - Level of education attained, including any training in specialized areas such as capital markets, information systems, fiduciary activities, and subsidiary activities.

- Significant banking industry audit experience, including specialized areas.

- Certification as a chartered bank auditor, certified internal auditor, etc.

- Their commitment to a program of continuing education and professional development.

4. If, in performing the preceding "Personnel" steps and the following "Processes" steps, there is sufficient reason to question the external auditor's independence, objectivity, or competence, discuss the situation with OCC district management, the Chief Accountant's office, and/or the Chief Counsel's department.

   - If appropriate, request through the bank that additional appropriate working papers be made available or meet with the external auditor to discuss the situation.

   - If it is determined that no reliance can be placed on the external auditor's work, discuss that assessment with the board of directors, bank management, and the affected party before finalizing the report of examination.

## Processes

Conclusion: The adequacy and reliability of the external auditors' work shows that management and the board have established (strong, satisfactory, weak) external audit processes.

Objective: Determine the adequacy and the reliability of work performed by the external auditors.

1. Determine whom the bank engages for performing the bank's external audit, i.e., CPA, certified information system auditor (CISA), or other independent parties.

2. Obtain copies of:

   - ☐ Engagement letters.
   - ☐ Annual reports.
   - ☐ Other external audit reports, including audit reports that the internal auditors may have participated in or relied on to any extent, such as AICPA SAS 70 ("Reports on the Processing of Transactions by Servicing Organizations") audits.
   - ☐ Letters to management.

3. Read the engagement letter covering activities of external auditors for statement certification, operational reviews, or appraisal of the internal audit function. Determine whether the letter addresses the following:

   - Purpose and scope of the audit.
   - Period to be covered by the audit.
   - Reports expected to be rendered.
   - Any limits on the scope of the audit.
   - Examiner access to work papers.

4. Determine the type of opinion (unqualified, qualified, adverse, or disclaimer) rendered by an IPA from an audit of the institution's financial statements.

   - If other than an unqualified opinion on the bank's financial statements has been issued, find out why.

5. Review the SAS 70 report rendered, if applicable. Determine how reliable the report is in assessing overall audit effectiveness. An SAS 70 report should not be the sole factor in assessing overall audit effectiveness. Consider:

   - The scope of the audit, i.e., whether the auditor

     – Tested controls at the institution or at the service organization or
     – Obtained and reviewed the service organization's report on controls placed in operation and tests of operating effectiveness.

   If deemed appropriate, request through the bank to review work papers supporting auditor's conclusions.

6. Review the external auditor's evaluation of departmental internal controls and compare it with the control evaluations done by OCC examiners (including any examiner-prepared ICQs).

7. Determine whether internal accounting controls have any material weaknesses (AICPA SAS 60, "Communication of Internal Control Structure Related Matters Noted in an Audit", requires that CPAs disclose material weaknesses either in writing or orally).

   - Read the report of material weaknesses.
   - Discuss any other communication between bank management and representatives of the accounting firm.

8. Obtain and review the list of audit differences or adjusting journal entries made and any list of waived adjustments. Determine whether such differences or entries are normal recurring accruals or indicate inadequate accounting records.

9. Request, through bank management, to review appropriate external audit work papers if the preceding steps disclose problems or issues with the external audit or if the examiner becomes aware of information that raises questions about the external audit program's adequacy. The following situations should trigger a review of external audit work papers:

   - Bank reliance on external audit in lieu of an internal audit program.
   - Unexpected or sudden change in the external auditor.
   - Significant changes in the external audit program.
   - Significant safety and soundness concerns.
   - Issues about the independence, objectivity, or competence of the external auditor.

   **Note:** IPAs for banks subject to 12 CFR 363 must agree to provide OCC examiners access to their work papers. For banks not subject to 12 CFR 363, examiners should work closely with the bank and the external auditor to access appropriate work papers.

10. Determine whether work papers disclose that specific program steps, calculations, or other evidence supports the procedures and

conclusions set forth. Given the prospect of minimal individual audit work program work papers, it may be beneficial to initially request to see the auditor's planning documents.

11. If, after performing the preceding steps, concerns remain about the adequacy of external audit, internal controls, or financial control integrity, the examiner should perform applicable **verification procedures** or complete appropriate **internal control questionnaires**.[21] If deemed appropriate, the examiner may request that the bank perform or ask its external auditor to perform verification procedures for areas that contain weaknesses or deficiencies.

12. Arrange through the bank to meet with the external auditor. Consider the following possible topics for discussion:

    - Examination and audit results or significant audit findings.
    - Upcoming audit and examination activities.
    - Reports, management letters, or other documents issued by the auditors.
    - Assigned audit staff experience and familiarity with banking and bank auditing, particularly in specialized areas.
    - Any other pertinent information.

## Controls

Conclusion: The board of directors and management (have/have not) established effective control systems for external audits.

Objective: Evaluate the adequacy of systems designed to monitor and assess control systems. Determine whether the board and management have instituted controls that are appropriate for the type and level of risks arising from the external audit function.

1. Review board or audit committee minutes, or summaries thereof, and determine whether the following is noted:

[21] Verification procedures are required in certain situations. See "Supervisory Process and Validation" section of this booklet for specific details.

- Formal approval of the external audit program and schedule, or reasons supporting any decision to forgo an external audit program.

- The monitoring of audit reports to determine whether approved programs and schedules are followed.

- The results of any vote taken regarding external audit.

- Confirmation that the audit committee reviewed external audit reports with management and the external auditors.

- Discussion of the external auditor's independence.

2. Trace the distribution of the external audit reports to determine whether the external auditor reports to the board or audit committee.

3. Determine whether external audit findings and recommendations are met with appropriate and timely responses.

4. Determine whether the activities of the external audit function are consistent with the institution's long-range goals and are responsive to its internal control and financial reporting needs.

5. Determine whether the board or its audit committee, at least annually, identifies the major risk areas in the institution's activities and assesses the extent of external auditing needed for each area.

# Overall Conclusions

**Conclusion: The quality of audit functions is (strong, satisfactory, weak)**

Objective: Determine the overall conclusions for the bank's audit functions.

1. Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. Areas to be covered should include:

   - The ability of the bank's audit processes to detect risk in bank operations.
   - The adequacy of audit policies, procedures, programs, and board's or audit committee's oversight.
   - Whether bank personnel operate in conformance with established policies.
   - The adequacy of information on the audit function available to management and the board of directors or its audit committee.
   - Significant areas of weaknesses identified by internal or external audits and management's progress in correcting those weaknesses.
   - Internal or external audit report findings not acted upon by management as well as any other concerns or recommendations resulting from the review of audit functions.
   - Recommended corrective actions, if applicable, and management's commitments.

2. Determine how the quality of the audit function's risks affect the aggregate level and direction of OCC risk assessments. Examiners should refer to guidance provided under the OCC's risk assessment programs for large banks and community banks.

3. Determine, in consultation with the EIC, whether the risks identified are significant enough to merit bringing them to the board's attention in the report of examination.

   If so, prepare items for inclusion under the heading "Matters Requiring Attention" (MRA). MRA comments should address practices that (1) deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed or (2) result in substantive noncompliance with laws or internal policies or processes. The examiner should provide details regarding:

   - The problem's causes.
   - Consequences of inaction.
   - Management's commitment to corrective action.
   - The time frame for any corrective action and who is responsible for the action.

4. Include a comment on audits in the report of examination taking into consideration the requirements of 12 CFR 30. The comment should address:

   - Adequacy of audit policies, processes, personnel, control systems, overall audit programs, and board/audit committee oversight.

   - Significant problems discerned by the auditors that have not been corrected.

   - Any deficiencies or concerns reviewed with management, any corrective actions recommended by examiners, and management's commitment(s) to corrective actions.

5. Prepare a memorandum to update OCC audit work programs with any information that will facilitate future examinations. Make recommendations about the scope of the next audit review and determine whether audit findings should change the scopes of other area reviews.

6. Update the OCC databases, including rating screens/schedules.

- For fiduciary, information system/technology, and compliance examinations, update the applicable audit component rating and communicate audit findings/rating to the appropriate EIC for incorporation into the UITRS, URSIT, or compliance rating systems.

7. Organize and reference working papers in accordance with PPM 5400-8.

# Appendix A: Statutory and Regulatory Requirements

By law, national banks must adhere to certain requirements regarding internal and external auditing functions. These requirements ensure that banks operate in a safe and sound manner, accurately prepare their financial statements, and comply with other banking laws and regulations.

## Operational and Managerial Standards

In July 1995, the OCC issued 12 CFR 30, Safety and Soundness Standards, establishing operational and managerial standards for all national banks. Some of these standards are for internal audit systems. According to appendix A to 12 CFR 30, a national bank should have an internal audit system that is appropriate to the size of the bank and the nature and scope of its activities. The appendix states that the audit system should provides for:

- Adequate monitoring of the system of internal controls through an internal auditing function. For a bank whose size, complexity or scope of operations does not warrant a full-scale internal auditing function, a system of independent reviews of key internal controls may be used.

- Independence and objectivity.

- Qualified persons.

- Adequate testing and review of information systems.

- Adequate documentation of tests and findings and any corrective actions.

- Verification and review of management actions to address material weaknesses.

- Review by the bank's audit committee or board of directors of the effectiveness of the internal auditing systems.

### Federal Securities Laws

National banks and bank holding companies that have securities registered with the Securities and Exchange Commission (SEC) are subject to the SEC's regulations on financial statement form, content, and other requirements.

17 CFR 210.2-01 addresses the qualifications and independence of independent public accountants (IPAs) engaged to perform services for companies with a class of securities registered pursuant to the Securities Exchange Act of 1934. CPAs must be duly registered and in good standing under the laws of the place of his/her residence or principal office. Public accountants must be in good standing and entitled to practice as such under the laws of the place of his/her residence or principal office. The SEC considers an accountant to lack independence when:

- During the period of the accountant's professional engagement to examine the financial statements being reported on or at the date of the report, the accountant, the accountant's firm, or another member of the firm had, or was committed to acquire, any direct financial interest or any material indirect financial interest in the company being examined; or

- During the period of the accountant's professional engagement to examine the financial statements being reported on, at the date of the report, or during the period covered by the financial statements, the accountant, the accountant's firm, or another member of the firm was connected as a promoter, underwriter, voting trustee, director, officer, or employee of the company being examined.

17 CFR 210.10-01, Interim Financial Statements, requires that IPAs must review interim financial statements included in a company's quarterly 10-Q reports using procedures in SAS 71, "Interim Financial Information."

17 CFR 229.306, Audit Committee Report, requires disclosures relating to the functioning of corporate audit committees. As part of proxy and information statements for meetings at which directors are to be elected, an audit committee report must be made which states whether the audit committee:

- Reviewed and discussed audited financial statements with management.

- Discussed with the company's IPA the matters required to be discussed by SAS 61, "Communication with Audit Committees."

- Received the written disclosures and the letter from the IPA (as required by Independence Standards Board Standard No. 1, "Independence Discussions with Audit Committees"), and discussed the IPA's independence with the IPA.

- After taking the preceding actions, recommended to the board of directors that the audited financial statements be included in the company's annual report.

Section 306 also requires that the name of each member of the company's audit committee appear below the above disclosures. In the absence of an audit committee, the names of the board committee performing the equivalent functions or the entire board must appear.

17 CFR 240, Section 14a-101, Information Required in a Proxy Statement, Item 7, Directors and Executive Officers, includes the following requirements if a registrant has an audit committee:

- Provide the information required by 17 CFR 229.306.
- State whether the board of directors has adopted a written charter for the audit committee.
- Include a copy of the written charter, if any, as an appendix to the proxy statement at least once every three years.

Section 14a-101 also includes other requirements depending on whether a company's securities are or are not listed on the New York Stock Exchange (NYSE) or American Stock Exchange (AMEX) or quoted on NASDAQ. If a bank is listed, the bank must disclose whether audit committee members are independent and, if a member is not independent, the nature of the relationship that makes the member not independent and the reasons for the board's determination. If a bank is not listed, the bank must disclose whether audit committee members are independent. For purposes of those requirements, the NYSE, AMEX, or National Association of Securities Dealers (NASD) definition of independence is used.

## Annual Independent Audit and Reporting Requirements

Following are the specific requirements of 12 CFR 363 (Part 363) on auditing, reporting, and audit committees. The requirements are applicable to all national banks with total assets of $500 million or more.

**Reports to Regulators.** National banks with $500 million or more in total assets must send the following reports to the FDIC and the appropriate OCC supervisory office:

- An annual report, due within 90 days after the fiscal year-end, consisting of:
  - Financial statements that include:
    - Comparative consolidated financial statements for each of the two most recent fiscal years prepared in accordance with generally accepted accounting principles and audited in accordance with generally accepted auditing standards by an independent public accountant; and
    - An audit report.
  - A management report that contains:
    - A statement of management's responsibilities for financial statements, establishing and maintaining an internal control structure and procedures for financial reporting, and complying with safety and soundness laws concerning loans to insiders and dividend restrictions;
    - Management's assessment of the effectiveness of the bank's internal control structure and procedures for financial reporting as of the end of the fiscal year (internal controls that safeguard assets, such as loan underwriting and documentation standards, must be considered) and the bank's compliance with designated laws and regulations during the most recent fiscal year.
  - A report by the independent public accountant attesting to management's assertions regarding internal control structure and procedures for financial reporting. The attestation is to be made in accordance with generally accepted standards for attestation engagements.
- Management letters and certain reports prepared for the bank, due 15 days after they are received, that include:

- Audit reports and any qualification to the audit reports;
- Any management letter; and
- Any other reports, including attestation reports, from the independent public accountant.
- A notification of the selection, change, or termination of the bank's independent public accountant, due within 15 days after the event. The report must include a statement of the reasons in sufficient detail for the examiner to evaluate the decision.

Independent public accountants for covered banks must file a report of termination of services, due within 15 days of the event. The report must be filed with the FDIC and the appropriate OCC supervisory office.

**Filing Reports.** Covered national banks, including covered branches of foreign banks, are required to file **two** copies of each required report at each of **two** locations the appropriate OCC supervisory office and the appropriate FDIC regional office. Of the OCC's copies, one will be maintained at the supervisory office, and the other will be forwarded to the bank's portfolio manager. The exception to this rule is the independent accountant's peer review report, which is required to be filed only with the FDIC.

**Disclosing Reports.** Annual reports required by Part 363 are available to anyone, from the bank, upon request. However, the OCC may designate certain information as privileged and confidential; such information may not be available to the public.

The peer review report is also publicly available. The list of clients subject to Part 363, however, is exempt from public disclosure.

**Reports to Independent Accountants.** Every covered national bank also must provide its independent public accountant with copies of the following reports:

- Its most recent OCC examination report and related correspondence;

- Its most recent Reports of Condition and Income or Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks; and

- Any supervisory memoranda of understanding, written agreements, requests for corrective action, notice of intent to commence an action,

record of enforcement action taken, or notice of change in the bank's prompt corrective action capital category during the audit period.

**Reports to the FDIC Only.** Independent public accountants for covered national banks must file the following reports with the Washington office of the FDIC:

- A peer review report for each covered bank or, if no peer review has been performed, a statement of the accountant's enrollment in a peer review program. This report is due within 15 days of receipt, or prior to commencing any services under Part 363; and

- A list of clients subject to Part 363, due at the accountant's option as a substitute for the peer review report or statement for each client.

**Special Reporting Situations.** *Consolidated Reporting by Holding Company Subsidiaries* -- A chart at the end of this appendix summarizes the responsibilities of holding company member banks. To simplify, any national bank that is a subsidiary of a holding company may, regardless of its size, file the audited consolidated financial statements of the holding company in place of separate financial statements.

All other report and notice requirements of the rule may be satisfied at the holding company level if:

- The bank has assets of less than $5 billion **or** of $5 billion or more with a composite CAMELS rating of 1 or 2, and

- The holding company provides the bank with comparable services and functions for other required reports and notices by:

  – Preparing reports used by subsidiary national banks to meet Part 363 requirements,

  – Having an audit committee that meets Part 363 requirements appropriate to its largest subsidiary bank, and

  – Preparing and submitting reports on internal control and compliance with designated laws based on the activities and operations of all subsidiary banks.

*Reporting by Insured U.S. Branches of Foreign Banks* -- Under the guidelines, insured branches of foreign banks may satisfy the financial statement requirement by filing:

- Audited balance sheets that also disclose information about financial instruments with off-balance-sheet risk;

- Audited call report schedules RAL and L of form FFIEC 002 (the Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks); **or**

- Consolidated financial statements of the parent company, if approved in writing by the OCC's appropriate supervisory office. Since consolidated financial statements do not necessarily provide relevant information about the branch, requests should be considered only in rare and unusual circumstances and any approvals should cover only a specified time period.

*Reporting by Merged or Consolidated Institutions* -- Insured national banks that had more than $500 million in total assets at the beginning of their fiscal year, but that no longer exist as a separate entity at the end of their fiscal year, have no responsibility under this rule to file reports due after the date they cease to exist.

A covered bank that merged into another institution after the end of the fiscal year but before its annual report and other reports must be filed under this rule should still submit reports to the FDIC and the appropriate OCC supervisory office.

National banks should consult with its OCC supervisory office concerning the statements and reports that would be required under such circumstances.

**Audit Committee Requirements.** National banks with total assets of $500 million or more must have independent audit committees that meet the following standards:

- The committee must be made up entirely of outside directors of the bank.

- The members must be independent of the management of the bank. The guidelines accompanying the Part 363 rule outline factors that should be considered in determining independence.

NOTE: Exceptions to the independent audit committee membership requirements may be granted in certain circumstances. Some insider directors may be allowed to serve on the audit committee if the OCC determines that the bank has encountered a hardship in retaining and recruiting competent outside directors. However, in no circumstances may the audit committee be made up of less than a majority of outside directors. Exceptions to the independent membership requirement should be rare and should be approved by the OCC's Office of the Chief Accountant.

- The committee's duties must include reviewing the basis of the reports required under Part 363, with management and the independent public accountant.

For banks with total assets of more than $3 billion, the audit committee also must:

- Include at least two members with banking and related financial management expertise.

- Not include any "large customers" of the banks.

  Any individual or entity (including a controlling person of a company) whose relationship with the bank (credit or otherwise, direct or indirect) is so significant that termination of the relationship would materially and adversely affect the bank's financial condition or results of operations should be considered a "large customer."

- Have access to the committee's own outside counsel.

**Special Audit Committee Situations**. *Bank Holding Company Subsidiary Banks* -- For banks that are subsidiaries of a holding company, the audit committee requirement may be satisfied at the holding company level if:

- The bank has assets of less than $5 billion **or** of $5 billion or more with a CAMELS composite rating of 1 or 2, and

- The holding company provides the bank with comparable services and functions for required other reports and notices by:

– Preparing reports used by subsidiary banks to meet Part 363 requirements,

– Having an audit committee that meets Part 363 requirements appropriate to its largest subsidiary bank, and

– Preparing and submitting reports on internal control and compliance with designated laws based on the activities and operations of all subsidiary banks.

A holding company subsidiary bank must have its own audit committee if the bank has total assets of $5 billion or more and a CAMELS composite rating of 3 or worse.

A holding company subsidiary bank's audit committee may be composed of the same persons as the holding company's audit committee **only** if such persons are:

- Outside directors of the holding company and the bank subsidiary, and
- Independent of management of the holding company and the bank.

Even in such situations, each audit committee must meet and maintain separate minutes of its meetings.

*Branches of Foreign Banks* -- Because branches of foreign banks do not have separate boards of directors, the audit committee requirements do not apply. However, insured branches of foreign banks are encouraged to make a good faith effort to see that duties similar to those described for the audit committee are performed by persons whose experience is generally consistent with the requirements.

**Implementation.** Every covered national bank was required to have established an audit committee by November 2, 1993. If the bank's audit committee did not meet the independence or other applicable criteria at that time, the bank had until the next annual stockholders' meeting or July 2, 1994, whichever was earlier, to structure the committee to comply.

Insured national banks that subsequently become subject to Part 363 requirements must form an independent audit committee within four months of the beginning of the first fiscal year in which they are covered.
An insured national bank that becomes covered by the large bank requirements by growing to have total assets of more than $3 billion must ensure that its audit committee meets the additional requirements by the next annual meeting of stockholders, or within six months of the beginning of its fiscal year, whichever is earlier.

**Independent Accountant Eligibility Requirements.** The independent public accountant must satisfy certain requirements to perform an audit or attestation for a covered bank. Specifically, the accountant must:

- Be enrolled in an acceptable peer review program, and

- File the peer review report (or a statement certifying enrollment in a peer review program if no peer review has yet been completed) with the Registration and Disclosure Section of the FDIC Washington office.

The report or statement must be filed within 15 days after the accountant receives notice that the peer review has been accepted by the appropriate practice section or other governing group, or before commencing the audit, whichever is earlier.

Following are some forms that may be helpful when reviewing Part 363 requirements.

## Part 363 Applied to Subsidiary Banks

| Insured Depository Institutions–Subsidiaries of Holding Companies with Assets of: | Audit Committee Requirements* | Reporting Requirements |
|---|---|---|
| Less than $500 million | None** | None** |
| $500 million to $3 billion | Committee must consist entirely of independent outside directors and may be satisfied at the holding company level. | Annual report, including:<br>• Audited financial statements,<br>• Audit report,<br>• Management report, and<br>• Independent public accountant's report on the internal controls over financial reporting.<br><br>Requirement may be satisfied at the holding company level. |
| $3 billion to $5 billion<br><br>and<br><br>$5 billion or more and CAMELS composite rating of 1 or 2. | Committee must:<br>• Consist entirely of independent outside directors,<br>• Include members with banking and related financial management expertise,<br>• Have access to its own outside counsel, and<br>• Not include large customers of the bank.<br><br>Requirements may be satisfied at the holding company level. | |
| $5 billion or more and CAMELS composite rating of 3 or worse. | Committee requirements same as above, but must be satisfied at the bank level. | Banks may submit holding company financial statements and audit reports, but all other reports listed above must be at the bank level. |

* Exceptions to the independent outside member requirement may be made when the OCC determines the bank has encountered a hardship in retaining or recruiting a sufficient number of competent outside directors. However, the audit committee may not be made up of less than a majority of outside directors.

** However, the banking agencies continue to encourage all institutions, regardless of size, to have annual audits and to establish audit committees made up entirely of outside directors.

NOTE: The appropriate federal banking agency may require a bank with total assets of $9 billion or more to comply with requirements of Part 363 at the bank level if the agency determines that exemptions as noted above, if applied to the bank, would create a significant risk to the deposit insurance fund.

# Part 363 Annual Report Worksheet*

| Name of Reporting Institution or Holding Company | Charter No. |
|---|---|
| City and State | Date Received |
| Name and Address (City, State) of Independent Accountant | Year End |
| If Holding Company, Names and Addresses of Subsidiary Institution(s) subject to Part 363 (attach list if needed) | Date of Last Peer Review |
| | Reviewer |

ANNUAL REPORT (Check attachments)

☐ Financial Statements and Notes ☐ Audit Report ☐ Management Report

☐ Independent Public Accountant's Attestation on Internal Controls

REVIEWER Complete all sections and the following questions:

Describe any item in the report that may adversely influence the institution's safety and soundness (reference should be made to the discussion in following sections I and II.)

| AS A RESULT OF THIS REVIEW, IS ANY FOLLOW-UP ACTION REQUIRED OR CHANGE IN SUPERVISORY STRATEGY WARRANTED? | YES ☐ | NO ☐ |
|---|---|---|

If yes, attach a memorandum outlining your recommendations.

* A new copy of this worksheet should be prepared each year upon receipt of either the annual report or the Laws and Regulations Attestation Report. Review of any other reports received periodically should be recorded on the "Part 363 Periodic Reports Worksheet".

I. ANNUAL REPORT

AUDIT REPORT

Do the report and financial statements cover a holding company or an individual institution? HC ☐ INST ☐

Has the report been signed and dated? YES ☐ NO ☐

Does it have any explanatory paragraphs in addition to the three paragraphs of the standard auditor's report? YES ☐ NO ☐

If yes, briefly describe the matter(s) covered in these paragraphs.

FINANCIAL STATEMENTS AND NOTES

Compare the information presented in the audited financial statements and the most recent available financial information from call report or examination report. Describe and discuss any differences or changes material to the institution between significant items on the statements and the call or examination report.

Briefly describe any unusual transactions or valuation methods described in the financial statements and accompanying notes that may influence the institution's safety and soundness including, but not limited to, those in the following areas:

- Securities
- Derivatives
- Other Real Estate
- Related Party Transactions
- Pensions or Deferred Compensation Plans
- Business Combinations/Pushdown Accounting
- Loans and Leases
- Servicing Rights
- Allowance for Loan and Lease Losses
- Taxes
- Off-Balance-Sheet Activities
- Nontraditional Activities

MANAGEMENT REPORT

| | |
|---|---|
| Does the report cover a holding company or an individual institution? | HC ☐ INST ☐ |
| Has the report been signed by both the CEO and the CFO/Chief accounting officer? | YES ☐ NO ☐ |
| Does it state management's responsibilities for: | |
| Preparing financial statements? | YES ☐ NO ☐ |
| Establishing and maintaining an adequate internal control structure and procedures for financial reporting? | YES ☐ NO ☐ |
| Complying with designated laws and regulations? | YES ☐ NO ☐ |
| Does it assess the: | |
| Effectiveness of the aforementioned internal controls at the end of the most recent year? | YES ☐ NO ☐ |
| Compliance with the designated laws and regulations during the year? | YES ☐ NO ☐ |

Briefly describe any instances of ineffectiveness or noncompliance reported by management or apparent deficiencies in reporting.

INDEPENDENT PUBLIC ACCOUNTANT'S ATTESTATION ON INTERNAL CONTROLS

| | |
|---|---|
| Has the report been signed and dated? | YES ☐ NO ☐ |
| Does it indicate material weaknesses in the internal control structure and procedures for financial reporting? | YES ☐ NO ☐ |

If so, briefly describe:

# Part 363 Periodic Report Worksheet*

| | |
|---|---|
| Name of Reporting Institution or Holding Company | Charter No. |
| City and State | Date Received |
| Name and Address (City, State) of Independent Accountant | Year End |
| If Holding Company, Names and Addresses of Subsidiary Institution(s) subject to Part 363 (attach list if needed) | Date of Last Peer Review |
| | Reviewer |

REPORT FILED

☐ Change of Accountant Report ☐ Termination of Services Report

☐ Management Letter ☐ Other Report (Describe)

REVIEWER -- Complete the following sections:

Describe briefly any item in the report that may adversely influence the institution's safety and soundness.

AS A RESULT OF THIS REVIEW, IS ANY FOLLOW-UP ACTION REQUIRED OR CHANGE IN SUPERVISORY STRATEGY WARRANTED? YES ☐ NO ☐

If yes, attach a memorandum outlining your recommendations.

* A separate copy of this worksheet should be completed upon receipt of each periodic report received. The "Annual Report Worksheet" should be used for the annual report.

# Appendix B: Interagency Policy Statement on the Internal Audit Function and its Outsourcing

**December 22, 1997**

## INTRODUCTION

Effective internal control[1] is a foundation for the safe and sound operation of a banking institution or savings association (hereafter referred to as institution). The board of directors and senior managers of an institution are responsible for ensuring that the system of internal control operates effectively. Their responsibility *cannot* be delegated to others within the institution or to outside parties. An important element of an effective internal control system is an internal audit function. When properly structured and conducted, internal audit provides directors and senior management with vital information about weaknesses in the system of internal control so that management can take prompt, remedial action. The agencies' long-standing examination policies call for examiners to review an institution's internal audit function and recommend improvements if needed. In addition, more recently, the agencies adopted Interagency Guidelines Establishing Standards for Safety and Soundness, pursuant to Section 39 of the Federal Deposit Insurance Act (FDI Act).[2] Under these guidelines, each institution should have an internal audit function that is appropriate to its size and the nature and scope of its activities.

In addressing various quality and resource issues, many institutions have been engaging independent public accounting firms and other outside professionals (hereafter referred to as outsourcing vendors) to perform work that has been traditionally done by internal auditors. These arrangements are often called "internal audit outsourcing", "internal audit assistance", "audit co-sourcing",

---

[1] In summary, internal control is a process, brought about by an institution's board of directors, management and other personnel, designed to provide reasonable assurance that the institution will achieve the following internal control objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and, compliance with applicable laws and regulations. Internal control consists of five components that are a part of the management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. The effective functioning of these components is essential to achieving the internal control objectives.

[2] For national banks, appendix A to Part 30; for state member banks, appendix D to Part 208; for state nonmember banks, appendix A to Part 364; for savings associations, appendix A to Part 570.

and "extended audit services" (hereafter, collectively referred to as outsourcing).

Such outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the federal banking agencies have concerns that the structure, scope, and management of some internal audit outsourcing arrangements may not contribute to the institution's safety and soundness. Furthermore, the agencies want to ensure that these arrangements with outsourcing vendors do not leave directors and senior managers with the impression that they have been relieved of their responsibility for maintaining an effective system of internal control and for overseeing the internal audit function.

This policy statement sets forth some characteristics of sound practices for the internal audit function and the use of outsourcing vendors for audit activities. In addition, it provides guidance on how these outsourcing arrangements may affect an examiner's assessment of internal control. It also discusses the effect these arrangements may have on the independence of an external auditor who also is providing internal audit services to an institution. Finally, this statement provides guidance to examiners concerning their reviews of internal audit functions and related matters. This policy statement applies to bank holding companies and their subsidiaries, FDIC-insured banks and savings associations, and U.S. operations of foreign banking organizations.

## THE INTERNAL AUDIT FUNCTION

### Director and Senior Management Responsibilities

The board of directors and senior management are responsible for having an effective system of internal control - including an effective internal audit function - and for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility *cannot* be delegated to anyone else. They may, however, delegate the design, implementation and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others. In discharging their responsibilities, directors and senior management should have reasonable assurance that the system of internal control prevents or detects inaccurate, incomplete or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial and

regulatory reporting; and deviations from laws, regulations, and the institution's policies.

Some institutions have chosen to rely on so-called "management self-assessments" or "control self-assessments," wherein business line managers and their staff evaluate the performance of internal controls within their purview. Such reviews help to underscore management's responsibility for internal control, but they are not impartial. Directors and senior managers who rely too much on these reviews may not learn of control weaknesses until they have become costly problems - particularly if directors are not intimately familiar with the institution's operations. Therefore, institutions generally should also have their internal controls tested and assessed by units without business-line responsibilities, such as internal audit groups.

Directors should be confident that the internal audit function meets the demands posed by the institution's current and planned activities. Directors and senior managers should ensure that the following matters are reflected in their internal audit function.

*Structure.* Careful thought should be given to placement of the audit function in the institution's management structure. The function should be positioned so that directors have confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. Accordingly, the manager of internal audit should report directly to the board of directors or its audit committee, which should oversee the internal audit function.[3] The board or its audit committee should develop objective performance criteria to evaluate the work of the internal audit function.[4]

*Management, staffing, and audit quality.* The directors should assign responsibility for the internal audit function to a member of management (hereafter referred to as the manager of internal audit or internal audit manager) who understands the function and has no responsibilities for

[3] Institutions subject to Section 36 of the FDI Act must maintain independent audit committees (i.e., comprised of directors that are not members of management). For institutions not subject to an audit committee requirement, the board of directors can fulfill the audit committee responsibilities discussed in this policy statement.

[4] For example, the performance criteria could include the timeliness of each completed audit, comparison of overall performance to plan, and other measures.

operating the business. The manager of internal audit should be responsible for control risk assessments, audit plans, audit programs and audit reports.

- A control risk assessment (or risk assessment methodology) documents the internal auditor's understanding of the institution's significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line and potential risk due to control deficiencies. They should be updated as needed to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.

- The audit plan is based on the control risk assessment and includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.

- An audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.

- An audit report generally presents the purpose, scope and results of the audit, including findings, conclusions and recommendations. Work papers should be maintained that adequately document the work performed and support the audit report.

The manager of internal audit should oversee the staff assigned to perform the internal audit work and should establish policies and procedures to guide the audit staff.[5] The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective. Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Institute for Internal Auditors' (IIA) *Standards for the Professional Practice of Internal Auditing*. These standards address the independence, professional proficiency, scope of work, performance of audit work, and management of internal audit.

*Scope.* The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities. At least annually, the audit committee should

[5] The form and content of policies and procedures should be consistent with the size and complexity of the department and the institution: many policies and procedures may be communicated informally in small internal audit departments, while many larger departments require more formal and comprehensive written guidance.

review and approve the internal audit manager's control risk assessment and the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.[6]

*Communication.* To properly discharge their responsibility for internal control, directors and senior management should foster forthright communications and critical examination of issues so that they will have knowledge of the internal auditor's findings and operating management's solutions to identified internal control weaknesses. Internal auditors should report internal control deficiencies to the appropriate level of management as soon as they are identified. Significant matters should be promptly reported directly to the board of directors (or its audit committee) and senior management. In periodic meetings with management and the manager of internal audit, the audit committee should assess whether internal control weaknesses or other exceptions are being resolved expeditiously by management. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.

## U.S. Operations of Foreign Banking Organizations

The internal audit function of a foreign banking organization (FBO) should cover its U.S. operations in its risk assessments, audit plans, and audit programs. The internal audit of the U.S. operations normally is performed by its U.S. domiciled audit function, head-office internal audit staff, or some combination thereof. Internal audit findings (including internal control deficiencies) should be reported to the senior management of the U.S. operations of the FBO and the audit department of the head office. Significant, adverse findings also should be reported to the head office's senior management and the board of directors or its audit committee.

---

[6] Major changes in an institution's environment and conditions may compel changes to the internal control system and also warrant additional internal audit work. These include: (a) new management; (b) areas or activities experiencing rapid growth © new lines of business, products or technologies; (d) corporate restructurings, mergers and acquisitions; and (e) expansion or acquisition of foreign operations (including the impact of changes in the related economic and regulatory environments).

### Small Financial Institutions

An effective system of internal control, including an independent internal audit function, is a foundation for safe and sound operations, regardless of an institution's size. As discussed previously in this policy statement, Section 39 of the FDI Act requires each institution to have an internal audit function that is appropriate to its size and the nature and scope of its activities. The procedures assigned to this function should include adequate testing and review of internal controls and information systems.

It is management's responsibility to carefully consider the level of auditing that will effectively monitor the internal control system after taking into account the audit function's costs and benefits. For many institutions that have reached a certain size or complexity of operations, the benefits derived from a full-time manager of internal audit or auditing staff more than outweigh its costs. However, for certain smaller institutions with few employees and less complex operations, these costs may outweigh the benefits. Nevertheless, a small institution without an internal auditor can ensure that it maintains an objective internal audit function by implementing a system of independent reviews of key internal controls. The employee conducting the review of a particular function should be independent of the function and able to report findings directly to the board or audit committee.

## INTERNAL AUDIT OUTSOURCING ARRANGEMENTS[7]

### Examples of Arrangements

An outsourcing arrangement is a contract between the institution and an outsourcing vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. The services under contract can be limited to helping internal audit staff in an assignment for which they lack expertise. Such an arrangement is typically under the control of the institution's manager of internal audit and the outsourcing vendor reports to him or her. Institutions often use outsourcing vendors for audits of areas requiring more technical expertise, such as those of electronic data processing and capital markets activities. Such uses are often referred to as "internal audit assistance" or "audit co-sourcing."

[7] The guidance in the preceding section of this policy statement ("The Internal Audit Function") also applies to internal audit outsourcing arrangements.

Some outsourcing arrangements may require an outsourcing vendor to perform virtually all internal audit work. Under such an arrangement, the institution may maintain a manager of internal audit and a very small internal audit staff. The outsourcing vendor assists staff in determining risks to be reviewed, recommends and performs audit procedures as approved by the internal audit manager, and reports its findings jointly with the internal audit manager to either the full board or its audit committee.

**Additional Considerations for Internal Audit Outsourcing Arrangements**

Even when outsourcing vendors provide internal audit services, the board of directors and senior managers of an institution are responsible for ensuring that the system of internal control (including the internal audit function) operates effectively. When negotiating the outsourcing arrangement with an outsourcing vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of internal control can occur.

To clearly set forth its duties from those of the outsourcing vendor, the institution should have a written contract, often referred to as an engagement letter. At a minimum, the contract should:

- Set the scope and frequency of work to be performed by the vendor;
- Set the manner and frequency of reporting to senior management and directors about the status of contract work;
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found;
- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the work papers prepared by the outsourcing vendor;
- Specify the locations of internal audit reports and the related work papers;

- State that examiners will be granted immediate and full access to the internal audit reports and related work papers prepared by the outsourcing vendor;

- Prescribe the method for determining who bears the cost of consequential damages arising from errors, omissions and negligence; and

- State that outsourcing vendors that are subject to the independence guidance below will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee.

*Management.* Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the manager of internal audit in overseeing the outsourcing vendor.

*Communication.* Communication between the internal audit function and directors and senior management should not diminish because the bank engages an outsourcing vendor. All work by the outsourcing vendor should be well documented and all findings of control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report the outsourcing vendor's findings to directors and senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of "materiality," as the term is used in financial audits, is generally not a good indicator of which control weakness to report. For example, when evaluating an institution's compliance with laws and regulations, any exception may be important.

*Vendor Competence.* Before entering an outsourcing arrangement the institution should perform enough due diligence to satisfy itself that the outsourcing vendor has sufficient staff qualified to perform the contracted work. Because the outsourcing arrangement is a personal services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the outsourcing vendor and receive prior notice of staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to perform effectively its contractual obligations.

*Contingency Planning.* When an institution enters into an outsourcing arrangement (or significantly changes the mix of internal and external resources used by internal audit), it increases its operating risk. Because the arrangement might be suddenly terminated, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high risk areas. Planning for a successor to the prospective outsourcing vendor should be part of negotiating the latter's service contract.

## Independence of the External Auditor

*This section of the policy statement applies only to an outsourcing vendor who is a certified public accountant (CPA) and who performs a financial statement audit or some other service for the institution that requires independence under AICPA rules.*[8]

Many institutions engage certified public accounting firms to audit their financial statements and furnish other attestation services requiring independence. A certified public accounting firm that provides other services for its client (such as consulting, benefits administration or acting as an outsourcing vendor) risks compromising the independence necessary to perform attestation services. The professional ethics committee of the American Institute of Certified Public Accountants (AICPA) has issued rulings and interpretations specifically addressing whether a certified public accountant that furnishes both audit outsourcing and external audit or other attestation services to a client can still be considered independent.[9]

Section 36 of the FDI Act and associated regulations require management of every insured depository institution with total assets of at least $500 million to obtain an annual audit of its financial statements by an independent public accountant, report to the banking agencies on the effectiveness of the institution's internal controls over financial reporting and on the institution's

[8] Although outsourcing arrangements involving CPAs who are not performing external audit or attestation services for a client are not subject to this independence guidance, they are subject to the other sections of this policy statement.

[9] In May 1997, the AICPA and the Securities and Exchange Commission announced the formation of the Independence Standards Board (ISB), a private-sector body intended to establish independence standards for auditors of public companies. Any future standards established by the IS should be considered in initiating or evaluating outsourcing arrangements with CPAs.

compliance with designated laws and regulations (management report), and obtain a report from an external auditor attesting to management's assertion about these internal controls (internal control attestation report). In order to satisfy these requirements, the institution's board of directors must select an external auditor that will satisfy the independence requirements established by the AICPA, and relevant requirements and interpretations of the Securities and Exchange Commission.

Questions have been raised about whether external auditors who perform an audit of the institution's financial statements or provide any other service that requires independence can also perform internal audit services and still be considered independent. The federal banking agencies are concerned that outsourcing arrangements may involve activities that compromise, in fact or appearance, the independence of an external auditor.

The AICPA has issued guidance to CPAs (Interpretation 101-13 and related rulings) on independence that addresses these issues. Under Interpretation 101-13, the CPA's performance of services required by the outsourcing arrangement "would not be considered to impair independence with respect to [an institution] for which the [CPA] also performs a service requiring independence, provided that [the CPA or the CPA's firm] does not act or appear to act in a capacity equivalent to a member of [the institution's] management or as an employee." The interpretation lists activities that would be considered to compromise a CPA's independence. Included are activities that involve the CPA "authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client."[10]

---

[10] Other examples of outsourcing activities that would compromise a CPA's independence that are listed in Interpretation 101-13 include:

- Performing ongoing monitoring activities or control activities (i.e., reviewing loan originations as part of the client's approval process or reviewing customer credit information as part of the customer's sales authorization process) that affect the execution of transactions or ensure that transactions are properly executed, accounted for, or both and performing routine activities in connection with the client's operating or production processes that are equivalent to those of an ongoing compliance or quality control function;
- Reporting to the board of directors or audit committee on behalf of management or the individual responsible for the internal audit function;
- Preparing source documents on transactions;
- Having custody of assets;
- Approving or being responsible for the overall internal audit work plan, including the determination of the internal audit risk and scope, project priorities, and frequency of performance of audit procedures;
- Being connected with the client in any capacity equivalent to a member of client

Also, the AICPA's Ruling No.103 sets forth three criteria for evaluating the independence of a CPA who concurrently provides internal audit outsourcing services and the internal control attestation report under Section 36 of the FDI Act. One criterion requires that management "does not rely on [the CPA's] work as the primary basis for its assertion and accordingly has (a) evaluated the results of its ongoing monitoring procedures built into the normal recurring activities of the entity (including regular management and supervisory activities) and (b) evaluated the findings and results of the [CPA's] work and other separate evaluations of controls, if any." Accordingly, a CPA's independence would be impaired if the CPA provides the *primary* support for management's assertion on the effectiveness of internal control over financial reporting. A copy of the interpretation and rulings is attached to this policy statement.

*Agencies' Views on Independence.* The agencies believe that other actions compromise independence in addition to those in Interpretation 101-13. Such actions include:[11]

- Contributing in a decision-making capacity or otherwise actively participating (e.g., advocating positions or actions rather than merely advising) in committees, task forces, and meetings that determine the institution's strategic direction; and

- Contributing in a decision-making capacity to the design, implementation, and evaluation of new products, services, internal controls or software that are significant to the institution's business activities.

management or as an employee (for example, being listed as an employee in client directories or other client publications, permitting himself or herself to be referred to by title or description as supervising or being in charge of the client's internal audit function, or using the client's letterhead or internal correspondence forms in communications).

[11] The agencies believe that this guidance is consistent with the AICPA interpretation.

## EXAMINATION GUIDANCE

### Review of the Internal Audit Function and Outsourcing Arrangements

Examiners should have full and timely access to an institution's internal audit resources, including personnel, work papers, risk assessments, work plans, programs, reports, and budgets. A delay may require examiners to widen the scope of their examination work and may subject the institution to follow-up supervisory actions.

Examiners will assess the quality and scope of the internal audit work, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners will consider whether:

- The board of directors (or audit committee) promotes the internal audit manager's impartiality and independence by having him or her directly report audit findings to it;

- The internal audit function's risk assessment, plans and programs are appropriate for the institution's activities;

- The internal audit function is adequately managed to ensure that audit plans are met, programs are carried out, and results of audits are promptly communicated to interested managers and directors;

- The institution has promptly responded to identified internal control weaknesses;

- Management and the board of directors use reasonable standards when assessing the performance of internal audit;

- The internal audit plan and program have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures or systems;

- The activities of internal audit are consistent with the long-range goals of the institution and are responsive to its internal control needs; and

- The audit function provides high-quality advice and counsel to management and the board of directors on current developments in risk management, internal control, and regulatory compliance.

The examiner should assess the competence of the institution's internal audit staff and management by considering the education and professional background of the principal internal auditors.

*Additional Aspects of the Examiner's Review of Outsourcing Arrangements.* Examiners should also determine whether:

- The arrangement maintains or improves the quality of the internal audit function and the institution's internal control;

- Key employees of the institution and the outsourcing vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the outsourcing vendor are to be addressed;

- The scope of work is revised appropriately when the institution's environment, structure, activities, risk exposures or systems change significantly;

- The directors have ensured that the outsourced internal audit function is effectively managed by the institution;

- The arrangement with the outsourcing vendor compromises its role as external auditor; and

- The institution has performed sufficient due diligence to satisfy itself of the vendor's competence before entering into the outsourcing arrangement and has adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.

If the examiner's evaluation of the outsourcing arrangement indicates that the outsourcing arrangement has diminished the quality of the institution's internal audit function, the examiner should consider adjusting the scope of the examination. The examiner also should bring that matter to the attention of senior management and the board of directors and consider it in the institution's management and composite ratings.

### Concerns about Auditor Independence

When an examiner's initial review of an outsourcing arrangement raises doubts about the external auditor's independence, the examiner first should ask the institution and the external auditor to demonstrate that the arrangement has not compromised the auditor's independence. If the examiner's concerns are not adequately addressed, the examiner should discuss the matter with appropriate agency staff.

If the agency's staff concurs that the independence of the external auditor appears to be compromised, the examiner will discuss his or her findings and the actions the agency may take with the institution's senior management, board of directors (or audit committee), and the external auditor. These actions may include referring the external auditor to the state board of accountancy and the AICPA for possible ethics violations, and barring the external auditor from engagements with regulated institutions. Moreover, the agency may conclude that the organization's external auditing program is inadequate and that it does not comply with auditing and reporting requirements, including Section 36 of the FDI Act and related guidance and regulations.

## AICPA Professional Rulings and Interpretations Referenced in the Interagency Policy Statement[12]

### RULINGS UNDER RULE OF CONDUCT 101

### 103 Member Providing Attest Report on Internal Controls

**.206** *Question* -- If a member or a member's firm (member) provides extended audit services for a client in compliance with interpretation 101- 13 [ET section 101.15], would the member be considered independent in the performance of an attestation engagement to report on the client's assertion regarding the effectiveness of its internal control over financial reporting?

[12] AICPA Professional Standards, copyright © 1996, American Institute of Certified Public Accountants, Inc.

**.207** *Answer* -- Independence would not be impaired with respect to the issuance of such a report if all of the following conditions are met:

1. The member's activities have been limited in a manner consistent with interpretation 101- 13 [ET section 101. 15].

2. Management has assumed responsibility to establish and maintain internal control.

3. Management does not rely on the member's work as the primary basis for its assertion and accordingly has (a) evaluated the results of its ongoing monitoring procedures built into the normal recurring activities of the entity (including regular management and supervisory activities) and (b) evaluated the findings and results of the member's work and other separate evaluations of controls, if any.

### 104 Member Providing Operational Auditing Services

**.208** *Question* -- As part of an extended audit engagement, a member or member's firm (member) may be asked to review certain of the client's business processes, as selected by the client, for how well they function, their efficiency, or their effectiveness. For example, a member may be asked to assess whether performance is in compliance with management's policies and procedures, to identify opportunities for improvement, and to develop recommendations for improvement or further action for management consideration and decision making. Would the member's independence be considered to be impaired in performing such a service?

**.209** *Answer* -- The member's independence would not be considered to be impaired provided that during the course of the review the member does not act or appear to act in a capacity equivalent to that of a member of client management or of an employee. The decision as to whether any of the member's recommendations will be implemented must rest entirely with management.

### 105 Frequency of Performance of Extended Audit Procedures

**.210** *Question* -- In providing extended audit services, would the frequency with which a member performs an audit procedure impair the member's independence?

**.211** *Answer* -- The independence of the member or member's firm would not be considered to be impaired provided that the member's activities have been limited in a manner consistent with interpretation 101-13 [ET section 101.15] and the procedures performed constituted separate evaluations of the effectiveness of the ongoing control and monitoring activities/procedures that are built into the client's normal recurring activities.

## INTERPRETATION 101-13 UNDER RULES OF CONDUCT 101: EXTENDED AUDIT SERVICES

**.101-13 -- Extended audit services.** A member or a member's firm (the member) may be asked by a client, for which the member performs a professional service requiring independence, to perform extended audit services. These services may include assistance in the performance of the client's internal audit activities and/or an extension of the member's audit service beyond the requirements of generally accepted auditing standards (hereinafter referred to as "extended audit services").

A member's performance of extended audit services would not be considered to impair independence with respect to a client for which the member also performs a service requiring independence, provided that the member or his or her firm does not act or does not appear to act in a capacity equivalent to a member of client management or as an employee.

The responsibilities of the client, including its board of directors, audit committee, and management, and the responsibilities of the member, as described below, should be understood by both the member and the client. It is preferable that this understanding be documented in an engagement letter that indicates that the member may not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee.

A member should be satisfied that the client understands its responsibility for establishing and maintaining internal control and directing the internal audit function, if any. As part of its responsibility to establish and maintain internal control, management monitors internal control to assess the quality of its performance over time. Monitoring can be accomplished through ongoing activities, separate evaluations or a combination of both.

Ongoing monitoring activities are the procedures designed to assess the quality of internal control performance over time and that are built into the normal recurring activities of an entity and include regular management and supervisory activities, comparisons, reconciliations and other routine actions. Separate evaluations focus on the continued effectiveness of a client's internal control. A member's independence would not be impaired by the performance of separate evaluations of the effectiveness of a client's internal control, including separate evaluations of the client's ongoing monitoring activities.

The member should understand that, with respect to the internal audit function, the client is responsible for:

5. Designating a competent individual or individuals, preferably within senior management, to be responsible for the internal audit function.

- Determining the scope, risk and frequency of internal audit activities, including those to be performed by the member providing extended audit services.

- Evaluating the findings and results arising from the internal audit activities, including those performed by the member providing extended audit services.

- Evaluating the adequacy of the audit procedures performed and the findings resulting from the performance of those procedures by, among other things, obtaining reports from the member.

The member should be satisfied that the board of directors and/or audit committee is informed of roles and responsibilities of both client management and the member with respect to the engagement to provide extended audit services as a basis for the board of directors and/or audit committee to establish guidelines for both management and the member to follow in

carrying out these responsibilities and monitoring how well the respective responsibilities have been met.

The member should be responsible for performing the audit procedures in accordance with the terms of the engagement and reporting thereon. The day-to-day performance of the audit procedures should be directed, reviewed, and supervised by the member. The report should include information that allows the individual responsible for the internal audit function to evaluate the adequacy of the audit procedures performed and the findings resulting from the performance of those procedures. This report may include recommendations for improvements in systems, processes, and procedures. The member may assist the individual responsible for the internal audit function in performing preliminary audit risk assessments, preparing audit plans, and recommending audit priorities. However, the member should not undertake any responsibilities that are required, as described above, to be performed by the individual responsible for the internal audit function.

Performing procedures that are generally of the type considered to be extensions of the member's audit scope applied in the audit of the client's financial statements, such as confirming of accounts receivable and analyzing fluctuations in account balances, would not impair the independence of the member or the member's firm even if the extent of such testing exceeds that required by generally accepted auditing standards.

The following are examples of activities that, if performed as part of an extended audit service, would be considered to impair a member's independence:

- Performing ongoing monitoring activities or control activities (for example, reviewing loan originations as part of the client's approval process or reviewing customer credit information as part of the customer's sales authorization process) that affect the execution of transactions or ensure that transactions are properly executed, accounted for, or both, and performing routine activities in connection with the client's operating or production processes that are equivalent to those of an ongoing compliance or quality control function.

- Determining which, if any, recommendations for improving the internal control system should be implemented.

- Reporting to the board of directors or audit committee on behalf of management or the individual responsible for the internal audit function.

- Authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client.

- Preparing source documents on transactions.

- Having custody of assets.

- Approving or being responsible for the overall internal audit work plan including the determination of the internal audit risk and scope, project priorities and frequency of performance of audit procedures.

- Being connected with the client in any capacity equivalent to a member of client management or as an employee (for example, being listed as an employee in client directories or other client publications, permit-ting himself or herself to be referred to by title or description as supervising or being in charge of the client's internal audit function, or using the client's letterhead or internal correspondence forms in communications).

The foregoing list is not intended to be all inclusive.[Effective Aug-31-96]

# Appendix C: Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations

**August 19, 1999**

## INTRODUCTION

The board of directors and senior managers of a banking institution or savings association (institution) are responsible for ensuring that the institution operates in a safe and sound manner. To achieve this goal and meet the safety and soundness guidelines implementing Section 39 of the Federal Deposit Insurance Act (FDI Act) (12 USC 1831p-1),[1] the institution should maintain effective systems and internal control[2] to produce reliable and accurate financial reports.

Accurate financial reporting is essential to an institution's safety and soundness for numerous reasons. First, accurate financial information enables management to effectively manage the institution's risks and make sound business decisions. In addition, institutions are required by law[3] to provide accurate and timely financial reports (e.g., Reports of Condition and Income [Call Reports] and Thrift Financial Reports) to their appropriate regulatory agency. These reports serve an important role in the *agencies*'[4] risk-focused supervision programs by contributing to their pre-examination planning, off-site monitoring programs, and assessments of an institution's capital adequacy and financial strength. Further, reliable financial reports are necessary for the institution to raise capital. They provide data to stockholders, depositors and other funds providers, borrowers, and potential investors on the company's financial position and results of operations. Such information is critical to effective market discipline of the institution**.**

---

[1] See 12 CFR Part 30 for national banks; 12 CFR Part 364 for state nonmember banks; 12 CFR Part 208 for state member banks; and 12 CFR Part 510 for savings associations.

[2] This Policy Statement provides guidance consistent with the guidance established in the "Interagency Policy Statement on the Internal Audit Function and its Outsourcing".

[3] See 12 USC 161 for national banks; 12 USC 1817a for state nonmember banks; 12 USC 324 for state member banks; and 12 USC 1464(v) for savings associations.

[4] Terms defined in Appendix A are italicized the first time they appear in this policy statement.

To help ensure accurate and reliable financial reporting, the agencies recommend that the board of directors of each institution establish and maintain an *external auditing program*. An external auditing program should be an important component of an institution's overall risk management process. For example, an external auditing program complements the *internal auditing* function of an institution by providing management and the board of directors with an independent and objective view of the reliability of the institution's *financial statements* and the adequacy of its financial reporting internal controls. Additionally, an effective external auditing program contributes to the efficiency of the agencies' risk-focused examination process. By considering the significant *risk areas* of an institution, an effective external auditing program may reduce the examination time the agencies spend in such areas. Moreover, it can improve the safety and soundness of an institution substantially and lessen the risk the institution poses to the insurance funds administered by the Federal Deposit Insurance Corporation (FDIC).

This policy statement outlines the characteristics of an effective external auditing program and provides examples of how an institution can use an external auditor to help ensure the reliability of its financial reports. It also provides guidance on how an examiner may assess an institution's external auditing program. In addition, this policy statement provides specific guidance on external auditing programs for institutions that are holding company subsidiaries, newly insured institutions, and institutions presenting supervisory concerns.

The adoption of a *financial statement audit* or other specified type of external auditing program is generally only required in specific circumstances. For example, insured depository institutions covered by Section 36 of the FDI Act (12 USC 1831m), as implemented by Part 363 of the FDIC's regulations (12 CFR part 363), are required to have an external *audit* and an *audit committee*. Therefore, this policy statement is directed toward banks and savings associations which are exempt from Part 363 (i.e., institutions with less than $500 million in total assets at the beginning of their fiscal year) or are not otherwise subject to audit requirements by order, agreement, statute, or agency regulations.

## OVERVIEW OF EXTERNAL AUDITING PROGRAMS

### Responsibilities of the Board of Directors

The board of directors of an institution is responsible for determining how to best obtain reasonable assurance that the institution's financial statements and *regulatory reports* are reliably prepared. In this regard, the board is also responsible for ensuring that its external auditing program is appropriate for the institution and adequately addresses the financial reporting aspects of the significant risk areas and any other areas of concern of the institution's business.

To help ensure the adequacy of its internal and external auditing programs, the agencies encourage the board of directors of each institution that is not otherwise required to do so to establish an audit committee consisting entirely of *outside directors*.[5] However, if this is impracticable, the board should organize the audit committee so that outside directors constitute a majority of the membership.

### Audit Committee

The audit committee or board of directors is responsible for identifying at least annually the risk areas of the institution's activities and assessing the extent of external auditing involvement needed over each area. The audit committee or board is then responsible for determining what type of external auditing program will best meet the institution's needs (refer to the descriptions under "Types of External Auditing Programs").

When evaluating the institution's external auditing needs, the board or audit committee should consider the size of the institution and the nature, scope, and complexity of its operations. It should also consider the potential benefits of an audit of the institution's financial statements or an examination of the institution's internal control structure over financial reporting, or both. In addition, the board or audit committee may determine that additional or specific external auditing procedures are warranted for a particular year or several years to cover areas of particularly high risk or special concern. The

[5] Institutions with $500 million or more in total assets must establish an independent audit committee made up of outside directors who are independent of management. See 12 USC 1831m(g)(1) and 12 CFR 363.5.

reasons supporting these decisions should be recorded in the committee's or board's minutes.

If, in its annual consideration of the institution's external auditing program, the board or audit committee determines, after considering its inherent limitations, that an agreed-upon procedures/state-required examination is sufficient, they should also consider whether an *independent public accountant* should perform the work. When an independent public accountant performs auditing and attestation services, the accountant must conduct his or her work under, and may be held accountable for departures from, professional standards. Furthermore, when the external auditing program includes an audit of the financial statements, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial statements are presented fairly, in all material respects, in accordance with generally accepted accounting principles (GAAP). When the external auditing program includes an *examination of the internal control structure over financial reporting*, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial reporting process is subject to any material weaknesses.

Both the staff performing an internal audit function and the independent public accountant or other external auditor should have unrestricted access to the board or audit committee without the need for any prior management knowledge or approval. Other duties of an audit committee may include reviewing the independence of the external auditor annually, consulting with management, seeking an opinion on an accounting issue, and overseeing the quarterly regulatory reporting process. The audit committee should report its findings periodically to the full board of directors.

## EXTERNAL AUDITING PROGRAMS

### Basic Attributes

External auditing programs should provide the board of directors with information about the institution's financial reporting risk areas, e. g., the institution's internal control over financial reporting, the accuracy of its recording of transactions, and the completeness of its financial reports prepared in accordance with GAAP.

The board or audit committee of each institution at least annually should review the risks inherent in its particular activities to determine the scope of its external auditing program. For most institutions, the lending and investment securities activities present the most significant risks that affect financial reporting. Thus, external auditing programs should include specific procedures designed to test at least annually the risks associated with the loan and investment portfolios. This includes testing of internal control over financial reporting, such as management's process to determine the adequacy of the allowance for loan and lease losses and whether this process is based on a comprehensive, adequately documented, and consistently applied analysis of the institution's loan and lease portfolio.

An institution or its subsidiaries may have other significant financial reporting risk areas such as material real estate investments, insurance underwriting or sales activities, securities broker-dealer or similar activities (including securities underwriting and investment advisory services), loan servicing activities, or fiduciary activities. The external auditing program should address these and other activities the board or audit committee determines present significant financial reporting risks to the institution.

### Types of External Auditing Programs

The agencies consider an annual audit of an institution's financial statements performed by an independent public accountant to be the preferred type of external auditing program. The agencies also consider an annual examination of the effectiveness of the internal control structure over financial reporting or an audit of an institution's balance sheet, both performed by an independent public accountant, to be acceptable alternative external auditing programs. However, the agencies recognize that some institutions only have agreed-upon procedures/state-required examinations performed annually as their external auditing program. Regardless of the option chosen, the board or audit committee should agree in advance with the external auditor on the objectives and scope of the external auditing program.

*Financial Statement Audit by an Independent Public Accountant*. The agencies encourage all institutions to have an external audit performed in accordance with generally accepted auditing standards (GAAS). The audit's

scope should be sufficient to enable the auditor to express an opinion on the institution's financial statements taken as a whole.

A financial statement audit provides assurance about the fair presentation of an institution's financial statements. In addition, an audit may provide recommendations for management in carrying out its control responsibilities. For example, an audit may provide management with guidance on establishing or improving accounting and operating policies and recommendations on internal control (including internal auditing programs) necessary to ensure the fair presentation of the financial statements.

*REPORTING BY AN INDEPENDENT PUBLIC ACCOUNTANT ON AN INSTITUTION'S INTERNAL CONTROL STRUCTURE OVER FINANCIAL REPORTING.* Another external auditing program is an independent public accountant's examination and report on management's assertion on the effectiveness of the institution's internal control over financial reporting. For a smaller institution with less complex operations, this type of engagement is likely to be less costly than an audit of its financial statements or its balance sheet. It would specifically provide recommendations for improving internal control, including suggestions for compensating controls, to mitigate the risks due to staffing and resource limitations.

Such an attestation engagement may be performed for all internal controls relating to the preparation of annual financial statements or specified schedules of the institution's regulatory reports.[6] This type of engagement is

[6] Since the lending and investment securities activities generally present the most significant risks that affect an institution's financial reporting, management's assertion and the accountant's attestation generally should cover those regulatory report schedules. If the institution has trading or off-balance-sheet activities that present material financial reporting risks, the board or audit committee should ensure that the regulatory report schedules for those activities also are covered by management's assertion and the accountant's attestation. For banks and savings associations, the lending, investment securities, trading, and off-balance-sheet schedules (which do not address all of an institution's possible risks) consist of:

| Area | Reports of Condition and Income Schedules | Thrift Financial Report Schedules |
|---|---|---|
| Loans and Lease Financing Receivables | RC-C, Part I | SC, CF |
| Past Due and Nonaccrual Loans, Leases, and Other Assets | RC-N | PD |
| Allowance for Credit Losses | RI-B | SC, VA |
| Securities | RC-B | SC, SI, CF |
| Trading Assets and Liabilities | RC-D | SO, SI |
| Off-Balance-Sheet Items | RC-L | SI, CMR |

performed under generally accepted standards for attestation engagements (GASAE).[7]

*BALANCE SHEET AUDIT PERFORMED BY AN INDEPENDENT PUBLIC ACCOUNTANT*. With this program, the institution engages an independent public accountant to examine and report only on the balance sheet. As with the audit of the financial statements, this audit is performed in accordance with GAAS. The cost of a *balance sheet audit* is likely to be less than a financial statement audit. However, under this type of program, the accountant does not examine or report on the fairness of the presentation of the institution's income statement, statement of changes in equity capital, or statement of cash flows.

AGREED-UPON PROCEDURES/STATE-REQUIRED EXAMINATIONS. Some state-chartered depository institutions are required by state statute or regulation to have *specified procedures* performed annually by their directors or independent persons.[8] The bylaws of many national banks also require that some specified procedures be performed annually by directors or others, including internal or independent persons. Depending upon the scope of the engagement, the cost of agreed-upon procedures or a state-required examination may be less than the cost of an audit. However, under this type of program, the independent auditor does not report on the fairness of the institution's financial statements or attest to the effectiveness of the internal control structure over financial reporting. The findings or results of the procedures are usually presented to the board or the audit committee so that they may draw their own conclusions about the quality of the financial reporting or the sufficiency of internal control.

When choosing this type of external auditing program, the board or audit committee is responsible for determining whether these procedures meet the external auditing needs of the institution, considering its size and the nature, scope, and complexity of its business activities. For example, if an

---

[7] An attestation engagement is not an audit. It is performed under different professional standards than an audit of an institution's financial statements or its balance sheet.

[8] When performed by an independent public accountant, "specified procedures" and "agreed-upon procedures" engagements are performed under standards, which are different professional standards than those used for an audit of an institution's financial statements or its balance sheet.

institution's external auditing program consists solely of confirmations of deposits and loans, the board or committee should consider expanding the scope of the auditing work performed to include additional procedures to test the institution's high risk areas. Moreover, a financial statement audit, an examination of the effectiveness of the internal control structure over financial reporting, and a balance sheet audit may be accepted in some states and for national banks in lieu of agreed-upon procedures/state-required examinations.

### Other Considerations

TIMING. The preferable time to schedule the performance of an external auditing program is as of an institution's fiscal year-end. However, a quarter-end date that coincides with a regulatory report date provides similar benefits. Such an approach allows the institution to incorporate the results of the external auditing program into its regulatory reporting process and, if appropriate, amend the regulatory reports.

EXTERNAL AUDITING STAFF. The agencies encourage an institution to engage an independent public accountant to perform its external auditing program. An independent public accountant provides a nationally recognized standard of knowledge and objectivity by performing engagements under GAAS or GASAE. The firm or independent person selected to conduct an external auditing program and the staff carrying out the work should have experience with financial institution accounting and auditing or similar expertise and should be knowledgeable about relevant laws and regulations.

## SPECIAL SITUATIONS

### Holding Company Subsidiaries

When an institution is owned by another entity (such as a holding company), it may be appropriate to address the scope of its external audit program in terms of the institution's relationship to the consolidated group. In such cases, if the group's consolidated financial statements for the same year are audited, the agencies generally would not expect the subsidiary of a holding company to obtain a separate audit of its financial statements. Nevertheless, the board of directors or audit committee of the subsidiary may determine that its activities involve significant risks to the subsidiary that are not within

the procedural scope of the audit of the financial statements of the consolidated entity. For example, the risks arising from the subsidiary's activities may be immaterial to the financial statements of the consolidated entity, but material to the subsidiary. Under such circumstances, the audit committee or board of the subsidiary should consider strengthening the internal audit coverage of those activities or implementing an appropriate alternative external auditing program.

### Newly Insured Institutions

Under the FDIC Statement of Policy on Applications for Deposit Insurance, applicants for deposit insurance coverage are expected to commit the depository institution to obtain annual audits by an independent public accountant once it begins operations as an insured institution and for a limited period thereafter.

### Institutions Presenting Supervisory Concerns

As previously noted, an external auditing program complements the agencies' supervisory process and the institution's internal auditing program by identifying or further clarifying issues of potential concern or exposure. An external auditing program also can greatly assist management in taking corrective action, particularly when weaknesses are detected in internal control or management information systems affecting financial reporting.

The agencies may require a financial institution presenting safety and soundness concerns to engage an independent public accountant or other independent external auditor to perform external auditing services.[9] Supervisory concerns may include:

- Inadequate internal control, including the internal auditing program;
- A board of directors generally uninformed about internal control;
- Evidence of insider abuse;
- Known or suspected defalcations;
- Known or suspected criminal activity;

[9] The Office of Thrift Supervision requires an external audit by an independent public accountant for savings associations with a composite rating of 3, 4, or 5 under the Uniform Financial Institution Rating System, and on a case-by-case basis.

- Probable director liability for losses;
- The need for direct verification of loans or deposits;
- Questionable transactions with affiliates; or
- The need for improvements in the external auditing program.

The agencies may also require that the institution provide its *appropriate supervisory office* with a copy of any reports, including management letters, issued by the independent public accountant or other external auditor. They also may require the institution to notify the supervisory office prior to any meeting with the independent public accountant or other external auditor at which auditing findings are to be presented.

## EXAMINER GUIDANCE

### Review of the External Auditing Program

The review of an institution's external auditing program is a normal part of the agencies' examination procedures. An examiner's evaluation of, and any recommendations for improvements in, an institution's external auditing program will consider the institution's size; the nature, scope, and complexity of its business activities; its risk profile; any actions taken or planned by it to minimize or eliminate identified weaknesses; the extent of its internal audit program; and any compensating controls in place. Examiners will exercise judgment and discretion in evaluating the adequacy of an institution's external auditing program.

Specifically, examiners will consider the policies, processes, and personnel surrounding an institution's external auditing program in determining whether:

- The board of directors or its audit committee adequately reviews and approves external auditing program policies at least annually.

- The external auditing program is conducted by an independent public accountant or other independent auditor and is appropriate for the institution.

- The *engagement letter* covering external auditing activities is adequate.

- The report prepared by the auditor on the results of the external auditing program adequately explains the auditor's findings.

- The external auditor maintains appropriate independence regarding relationships with the institution under relevant professional standards.

- The board of directors performs due diligence on the relevant experience and competence of the independent auditor and staff carrying out the work (whether or not an independent public accountant is engaged).

- The board or audit committee minutes reflect approval and monitoring of the external auditing program and schedule, including board or committee reviews of audit reports with management and timely action on audit findings and recommendations.

**Access to Reports**

Management should provide the independent public accountant or other auditor with access to all examination reports and written communication between the institution and the agencies or state bank supervisor since the last external auditing activity. Management also should provide the accountant with access to any supervisory memoranda of understanding, written agreements, administrative orders, reports of action initiated or taken by a federal or state banking agency under section 8 of the FDI Act (or a similar state law), and proposed or ordered assessments of civil money penalties against the institution or an institution-related party, as well as any associated correspondence. The auditor must maintain the confidentiality of examination reports and other confidential supervisory information.

In addition, the independent public accountant or other auditor of an institution should agree in the engagement letter to grant examiners access to all the accountant's or auditor's work papers and other material pertaining to the institution prepared in the course of performing the completed external auditing program.

Institutions should provide reports[10] issued by the independent public accountant or other auditor pertaining to the external auditing program, including any management letters, to the agencies and any state authority in accordance with their appropriate supervisory office's guidance.[11] Significant developments regarding the external auditing program should be communicated promptly to the appropriate supervisory office. Examples of those developments include the hiring of an independent public accountant or other third party to perform external auditing work and a change in, or termination of, an independent public accountant or other external auditor.

## Appendix A — Definitions

*Agencies*. The agencies are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

*Appropriate supervisory office.* The regional or district office of the institution's primary federal banking agency responsible for supervising the institution or, in the case of an institution that is part of a group of related insured institutions, the regional or district office of the institution's federal banking agency responsible for monitoring the group. If the institution is a subsidiary of a holding company, the term "appropriate supervisory office" also includes the federal banking agency responsible for supervising the holding company. In addition, if the institution is state-chartered, the term "appropriate supervisory office" includes the appropriate state bank or savings association regulatory authority.

---

[10] The institution's engagement letter is not a "report" and is not expected to be submitted to the appropriate supervisory office unless specifically requested by that office.

[11] When an institution's financial information is included in the audited consolidated financial statements of its parent company, the institution should provide a copy of the audited financial statements of the consolidated company and any other reports by the independent public accountant in accordance with their appropriate supervisory office's guidance. If several institutions are owned by one parent company, a single copy of the reports may be supplied in accordance with the guidance of the appropriate supervisory office of each agency supervising one or more of the affiliated institutions and the holding company. A transmittal letter should identify the institutions covered. Any notifications of changes in, or terminations of, a consolidated company's independent public accountant may be similarly supplied to the appropriate supervisory office of each supervising agency.

*Audit*. An examination of the financial statements, accounting records, and other supporting evidence of an institution performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards (GAAS) and of sufficient scope to enable the independent public accountant to express an opinion on the institution's financial statements as to their presentation in accordance with generally accepted accounting principles (GAAP).

*Audit committee*. A committee of the board of directors whose members should, to the extent possible, be knowledgeable about accounting and auditing. The committee should be responsible for reviewing and approving the institution's internal and external auditing programs or recommending adoption of these programs to the full board.

*Balance sheet audit performed by an independent public accountant*. An examination of an institution's balance sheet and any accompanying footnotes performed and reported on by an independent public accountant in accordance with GAAS and of sufficient scope to enable the independent public accountant to express an opinion on the fairness of the balance sheet presentation in accordance with GAAP.

*Engagement letter*. A letter from an independent public accountant to the board of directors or audit committee of an institution that usually addresses the purpose and scope of the external auditing work to be performed, period of time to be covered by the auditing work, reports expected to be rendered, and any limitations placed on the scope of the auditing work.

*Examination of the internal control structure over financial reporting.* See Reporting by an Independent Public Accountant on an Institution's Internal Control Structure Over Financial Reporting.

*External auditing program*. The performance of procedures to test and evaluate high risk areas of a institution's business by an independent auditor, who may or may not be a public accountant, sufficient for the auditor to be able to express an opinion on the financial statements or to report on the results of the procedures performed.

*Financial statement audit by an independent public accountant.* See Audit.

*Financial statements*. The statements of financial position (balance sheet), income, cash flows, and changes in equity together with related notes.

*Independent public accountant*. An accountant who is independent of the institution and registered or licensed to practice, and holds himself or herself out, as a public accountant, and who is in good standing under the laws of the state or other political subdivision of the United States in which the home office of the institution is located. The independent public accountant should comply with the American Institute of Certified Public Accountants' (AICPA) Code of Professional Conduct and any related guidance adopted by the Independence Standards Board and the agencies. No certified public accountant or public accountant will be recognized as independent who is not independent both in fact and in appearance.

*Internal auditing*. An independent assessment function established within an institution to examine and evaluate its system of internal control and the efficiency with which the various units of the institution are carrying out their assigned tasks. The objective of internal auditing is to assist the management and directors of the institution in the effective discharge of their responsibilities. To this end, internal auditing furnishes management with analyses, evaluations, recommendations, counsel, and information concerning the activities reviewed.

*Outside directors*. Members of an institution's board of directors who are not officers, employees, or principal stockholders of the institution, its subsidiaries, or its affiliates, and who do not have any material business dealings with the institution, its subsidiaries, or its affiliates.

*Regulatory reports*. These reports are the Reports of Condition and Income (Call Reports) for banks, Thrift Financial Reports (TFRs) for savings associations, Federal Reserve (FR) Y reports for bank holding companies, and the H-(b)11 Annual Report for thrift holding companies.

*Reporting by an independent public accountant on an institution's internal control structure over financial reporting*. Under this engagement, management evaluates and documents its review of the effectiveness of the institution's internal control over financial reporting in the identified risk areas as of a specific report date. Management prepares a written assertion, which specifies the criteria on which management based its evaluation about the

effectiveness of the institution's internal control over financial reporting in the identified risk areas and states management's opinion on the effectiveness of internal control over this specified financial reporting. The independent public accountant is engaged to perform tests on the internal control over the specified financial reporting in order to attest to management's assertion. If the accountant concurs with management's assertion, even if the assertion discloses one or more instances of material internal control weakness, the accountant would provide a report attesting to management's assertion.

*Risk areas*. Those particular activities of an institution that expose it to greater potential losses if problems exist and go undetected. The areas with the highest financial reporting risk in most institutions generally are their lending and investment securities activities.

*Specified procedures.* Procedures agreed-upon by the institution and the auditor to test its activities in certain areas. The auditor reports findings and test results, but does not express an opinion on controls or balances. If performed by an independent public accountant, these procedures should be performed under generally accepted standards for attestation engagements (GASAE).

# Appendix D: Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners [1]

**July 23, 1992**

The federal bank and thrift regulatory agencies are issuing this policy statement to improve the coordination and communication between external auditors and examiners. This policy statement provides guidelines regarding information that should be provided by depository institutions to their external auditors and meetings between external auditors and examiners in connection with safety and soundness examinations.

## Coordination of External Audits and Examinations

In most cases, the federal bank and thrift regulatory agencies provide institutions with advance notice of the starting date(s) of full-scope or other examinations. When notified, institutions are encouraged to promptly advise their external auditors of the date(s) and scope of supervisory examinations in order to facilitate the auditors' planning and scheduling of audit work. The external auditors may also advise the appropriate regulatory agency regarding the planned dates for the auditing work on the institution's premises in order to facilitate coordination with the examiners.

Some institutions prefer that audit work be completed at different times from examination work in order to reduce demands upon their staff members and facilities. On the other hand, some institutions prefer to have audit work and examination work performed during similar periods in order to limit the effect of these efforts on the institutions' operations to certain times during the year. By knowing in advance when examinations are planned, institutions have the flexibility to work with their external auditors to schedule audit work concurrent with examinations or at separate times.

[1] The agencies issuing this policy statement are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

## Other Information Provided By the Institution

Consistent with prior practice, a depository institution should provide its external auditors with a copy of certain reports and supervisory documents including:

- The most recent regulatory Report of Condition (i.e., "Call Reports" for banks, and "Thrift Financial Reports" for savings institutions);

- The most recent examination report and pertinent correspondence received from its regulator(s);

- Any supervisory memorandum of understanding with the institution that has been put into effect since the beginning of the period covered by the audit;

- Any written agreement between a federal or state banking agency and the institution that has been put into effect since the beginning of the period covered by the audit; and

- A report of:

  – Any actions initiated or undertaken by a federal banking agency since the beginning of the period covered by the audit under certain subsections of Section 8 of the Federal Deposit Insurance Corporation Act,[2] or any similar action taken by an appropriate state bank supervisor under state law; and

  – Any civil money penalty assessed under any other provision of law with respect to the depository institution or any institution-affiliated party, since the beginning of the period covered by the audit.

[2] Section 112 of the Federal Deposit Insurance Corporation Act of 1991 includes a requirement that the institution provide its external auditors with a report of any action initiated or taken by a federal banking agency during the period under audit under subsection (a),(b),(c),(e),(g),(I),(s) or (t) of Section 8 of the Federal Deposit Insurance Act (12 USC 1817).

## External Auditor Attendance at Meetings Between Management and Examiners

Generally, the federal bank and thrift regulatory agencies encourage auditors to attend examination exit conferences upon completion of field work or other meetings between supervisory examiners and an institution's management or Board of Directors (or a committee thereof) at which examination findings are discussed that are relevant to the scope of the audit. When other conferences between examiners and management are scheduled (i.e., that do not involve examination findings that are relevant to the scope of the external auditor's work), the institution shall first obtain the approval of the appropriate federal bank or thrift regulatory agency in order for the auditor to attend the meeting. This policy does not preclude the federal bank and thrift regulatory agencies from holding meetings with the management of depository institutions without auditor attendance or from requiring that the auditor attend only certain portions of the meetings.

Depository institutions should ensure that their external auditors are informed in a timely manner of scheduled exit conferences and other relevant meetings with examiners and of the agencies' policies regarding auditor attendance at such meetings.

## Meetings and Discussions Between External Auditors and Examiners

An auditor may request a meeting with any or all of the appropriate federal bank and thrift regulatory agencies, that are involved in the supervision of the institution or its holding company during, or after completion of, examinations in order to inquire about supervisory matters relevant to the institution under audit. External auditors should provide an agenda in advance to the agencies that will attend these meetings. The federal bank and thrift regulatory agencies will generally request that management of the institution under audit be represented at the meeting. In this regard, examiners generally will only discuss with an auditor examination findings that have been presented to the depository institution's management.

In certain cases, external auditors may wish to discuss with regulators matters relevant to the institution under audit at meetings without the representation from the institution's management. External auditors may request such confidential meetings with any or all of the federal bank and thrift regulatory

agencies, and the agencies may also request such meetings with the external auditor.

### Confidentiality of Supervisory Information

While the policies of the federal bank and thrift regulatory agencies permit external auditors to have access to the previously mentioned information on depository institutions under audit, institutions and their auditors are reminded that information contained in examination reports, inspection reports, and supervisory discussions -- including any summaries or quotations -- is confidential supervisory information and must not be disclosed to any party without the written permission of the appropriate federal or thrift regulatory agency. Unauthorized disclosure of confidential supervisory information may subject the auditor to civil and criminal actions and fines and other penalties.

# Appendix E: Internal Audit Review Worksheet

This worksheet is designed as a tool to help examiners evaluate the quality of internal audit programs, work papers, and related reporting for individual bank departments, activities, products, or services. If completed, the worksheet should be shared with other examiners as appropriate to facilitate an overall internal audit assessment. Use of the worksheet is not mandatory.

Unit Audited: _____ Date of audit report: _____
Auditor in Charge: _____ Audit Frequency: _____
Audit Rating: _____ Agree w/Rating: ____ Y ____ N
Management Response: ____ Y ____ N Response Adequate: ____Y ____ N
Risk Rating: _____

| ***Scope*** | | |
|---|---|---|
| 1. Was the scope of the audit adequate? | ____ Yes<br>____ No | Why or why not: |
| | | |
| 2. Comment on quality of the planning document. | ____ Adequate<br>____ Inadequate<br>____ Not Applicable | Why: |
| | | |
| 3. Is the audit frequency appropriate relative to the level of risk in the area/unit? | ____ Yes<br>____ No | Why or why not: |
| | | |
| 4. Is any portion of this audit outsourced? | ____ All<br>____ Partial<br>____ Not Applicable | |
| a. If so, is the arrangement compliant with OCC 98-1? | ____ Yes<br>____ No | Why not: |
| b. If so, is the audit work of sufficient detail to draw appropriate conclusions? | ____ Yes<br>____ No | Why not: |
| | | |
| **Risk Assessment** | | |
| 5. Were risk assessment matrices used to describe the | ____ Yes<br>____ No | Why not: |

| | | |
|---|---|---|
| risk(s)? | | |
| a. If yes, were they sufficient? | ____ Yes<br>____ No | Why not: |
| | | |
| 6. Was risk assessment used to determine when to audit this area? | ____ Yes<br>____ No | Why not: |
| | | |
| 7. Was risk assessment used to determine the scope of the audit? | ____ Yes<br>____ No | Why not: |
| | | |
| 8. Is the risk assessment of this area adequate? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Work/Findings*** | | |
| 9. Were the audit program and procedures sufficient? | ____ Yes<br>____ No | Describe the deficiencies: |
| | | |
| 10. Were audit procedures performed to ensure compliance with applicable: | | |
| a. Policies | ____ Yes<br>____ No<br>____ Not Applicable | |
| b. Procedures? | ____ Yes<br>____ No<br>____ Not Applicable | |
| c. Plans? | ____ Yes<br>____ No<br>____ Not Applicable | |
| d. Laws/regulations? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 11. Were internal controls for the area sufficiently detailed? | ____ Yes<br>____ No | |
| | | |
| 12. Did the audit contain tests of administrative or operational: | | |

| | | |
|---|---|---|
| a. Controls? | ____Yes<br>____ No | |
| b. Policies? | ____ Yes<br>____ No | |
| c. Procedures? | ____ Yes<br>____ No | |
| | | |
| 13. Did the audit note the cause of deficiencies or symptoms of problems? | ____ Cause<br>____ Symptom<br>____ Both<br>____ Not Applicable | |
| | | |
| 14. Was a review of pertinent MIS performed as part of the audit? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| 15. What is the quality of the procedures documentation? | ____ High<br>____ Acceptable<br>____ Unacceptable | Support: |
| a. Are audit trails sufficient? | ____ Yes<br>____ No | Why not: |
| | | |
| 16. How well does the audit describe the risk represented in individual findings or groups of findings? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support: |
| | | |
| 17.If the area/unit is internally rated satisfactory, how well does the audit mitigate the existence of significant findings? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support: |
| | | |
| 18. Were all exceptions or weaknesses in the audit WPs noted in the final audit report? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| 19. Were the internal auditors, including outsourced vendors, adequately trained and experienced to complete this program? | ____ Yes<br>____ No | How determined: |
| | | |

| | | |
|---|---|---|
| 20. How well does the auditor-in-charge (AIC) support the final audit rating? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support |
| | | |
| 21. Do you agree with the final rating? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| **Sampling** | | |
| 22. Did the auditor use statistical sampling? | ____ Yes<br>____ No<br>____ Not Applicable | |
| a. Was the population accurately defined? | ____ Yes<br>____ No | Why not: |
| b. Was the selection of the sampling method disclosed? | ____ Yes<br>____ No | Why not: |
| c. Were the sample selection techniques disclosed? | ____ Yes<br>____ No | Why not: |
| d. Were sample evaluation and reporting results criteria established? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Reports*** | | |
| 23. Does the audit report articulate the appropriate conclusions, findings, and recommendations? | ____ Yes<br>____ No | Why not: |
| | | |
| 24. Does the audit report address the root cause of problems and recommends or actions to correct problems? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 25. What level of management was notified of the audit findings? | | |
| a. Is this the appropriate level or person? | ____ Yes<br>____ No | If not, who: |
| | | |

| | | |
|---|---|---|
| 26. Does the AIC or supervisor make effective use of MIS and have periodic contact with area/unit management? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Follow-up*** | | |
| 27. Was there evidence that prior audit issues were properly followed up during the current audit? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 28. Was management's response to audit findings timely? | ____ Yes<br>____ No | |
| | | |
| 29. Was management's response to audit findings acceptable? | ____ Yes<br>____ No | Why not: |
| | | |
| 30. Are corrective action time frames included in management's response? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 31. How effective and timely are management's plans for addressing deficiencies? | ____ Adequate<br>____ Inadequate<br>____ Not Applicable | Why inadequate: |
| | | |
| 32. Are audit exceptions in this area sufficiently detailed on an exception tracking report? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| 33. Is there sufficient follow-up activity for high-risk areas/units or areas/units adversely rated? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| ***Quality Assurance*** | | |
| 34. Was the audit subject to a Quality Control Review? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |

| | | |
|---|---|---|
| | | |
| ***Meetings with Auditors*** | | |
| 35. Summarize any discussions with internal auditors or outsourced internal auditor vendors ( summary should include but not be limited to: participants, date, subject, conclusions or recommendations, and the participants' receptiveness and responses. | | |
| | | |
| ***Overall Conclusion*** | | |
| 36. Should the OCC adjust its strategy for this bank/business unit based upon your review of the audit reports, memos, and WPs? | ____ Yes<br>____ No | Why or why not and what adjustments should be made? |
| | | |
| 37. Provide any other information deemed appropriate. | | |

# Appendix F: Audit Function Questionnaire

This audit function questionnaire (AFQ) is designed as a tool to help examiners evaluate a bank's internal or external audit functions. Its use is not mandatory. Examiners should complete the AFQ only if they determine that the auditors are both competent and independent. Based on the auditors' work and the answers to the specific audit function questions, the examiner can then determine which verification procedures he or she considers necessary to perform.

The following audit function questions are reflective of a simplistic banking environment. Differing banking environments and roles of bank personnel in assessing overall controls and other variables affect the kinds of audit procedures that may be appropriate for a bank. Examiners should refer to individual booklets of the *Comptroller's Handbook* for more detailed audit requirements for complex or specialty areas or activities. In many cases, for external audits, all of the audit function questions may not be applicable to the type and extent of the audit/review conducted. Review reports, programs and audit work papers to answer the audit function questions. Where appropriate, supporting documentation and pertinent information should be retained or noted under comments.

For the following areas, has the internal auditor (or external auditor if deemed appropriate) within a reasonable audit cycle:

**Cash Accounts**

1. Counted cash on hand (including confirmation of incoming or outgoing cash shipments)?

2. Determined the propriety of amount and classification for cash items?

3. Confirmed clearings and reviewed all incoming returned items for some period after the date clearings were confirmed?

4. Checked adherence to procedures for maintaining records in accordance with 31 CFR 103.21, 03.22, 103.23, 103.25, 103.27, 103.29, 103.32, 103.33, 103.34, 103.35, 103.36, and 103.37?

5. Checked adherence to the provisions of 31 CFR 103, performing the following for:

   a. Reporting Requirements: Determined coverage requirements that include a review of a teller's work and of forms 4789 and 4790?

   b. Record keeping Activities: Tested the bank's adherence to the in-house record retention schedule? This schedule should meet the requirements of the regulation.

   c. Exemptions: Ascertained that the bank maintains a list of exempt customers?

      **S** Tested the reasonableness of the exemptions granted?

      **S** Ascertained that the bank completes and maintains the exemption certification?

   d. Foreign Accounts: Ascertained that the bank has filed Form 90-22.1, declaring interest in a foreign financial account?

   e. Volume of Cash Movements: Reviewed cash control records and traced any apparently large or unusual cash movements to or from a department or branch?

6. Checked adherence to 12 CFR 21.21 in establishing a written Bank Secrecy Act compliance program approved by the board of directors?

**Due From Banks**

1. Tested bank reconcilement including the Federal Reserve bank?

2. Received cut-off bank statements as of the examination date and an appropriate date subsequent to the examination date for use in testing bank reconcilement?

3. Reviewed all returned items for an appropriate period subsequent to the examination date?

4. Confirmed due from banks--time accounts with the banks holding the deposits?

5. Determined accuracy and completeness of reports FR 2900 and FR 2950 submitted to the Federal Reserve for calculation of required reserve balances?

**Investments**

1. Confirmed held-to-maturity and available-for-sale securities balances (including physical count of securities located at the bank, and confirmation of bank ownership and control of securities held in custody outside the bank or in transit)?

2. Determined the book and market value of investment securities?

3. Determined the gain and loss of investment securities sold during the period?

4. Reviewed the accrued interest accounts and tested computation of interest income?

5. Checked for compliance with the FFIEC "Supervisory Policy Statement on Investment Securities and End-User Derivatives (OCC 98-20)?

6. Checked for compliance with the repurchase agreement provision of the Government Securities Act for non-dealer banks (15 USC 78o-5)?

7. Checked for compliance with laws and regulations applicable to those banks engaging in the purchase or sale of securities instruments for their own account or for the account of customers (including furnishing commodity advice to customers)?

**Retail Non-Deposit Investment Sales**

1. Checked monitoring and resolution of customer complaints?

2. Tested customer accounts for proper disclosures, advertising, and suitability determination?

3. Checked for conflicts of interest?

4. Reviewed the bank's compensation program for retail non-deposit investment product sales?

5. If the bank has a separate compliance program for retail non-deposit investment product sales, did audit review the adequacy of the compliance program?

6. Where the bank offers retail non-deposit investment products through an independent third party vendor, did audit review vendor adherence to the governing agreement?

7. Ascertained that sales activities were in keeping with established policies and procedures, applicable laws and regulations, and the February 15, 1994 Interagency statement?

**Bank Derivatives**

(The level of internal auditor expertise should be consistent with the level of activity and degree of risk assumed by the bank. In some cases, banks may need to outsource audit coverage of derivative activities to ensure that the persons performing the audit work possess sufficient depth and experience.)

1. Assessed the adequacy and reasonableness of information obtained and used in risk management systems (market, credit, liquidity, and operations/systems)?

2. Validated the data integrity of significant market, liquidity, and risk management models?

3. Determined that contract documentation is properly maintained and safeguarded, and ascertained that legal counsel has properly reviewed documents?

4. Confirmed the effectiveness of internal control systems used for derivatives transaction processing and valuation?

5. Checked compliance with laws, rules, regulations, and proper accounting?

6. Ascertained that derivative activities are performed within the guidelines provided by bank policies and procedures?

7. Participated in the new product review process, approving the audit procedures developed for testing any new products or activities?

**Mortgage Banking Activities**

1. Tested book and fair-market values of mortgage servicing rights (MSR) and excess servicing fees received (ESFR) assigned to pools of loans?

2. Verified accuracy of hedge accounting?

3. Tested the accuracy of tracking systems by verifying that documentation was on hand, or in process of being received, for loans awaiting sales and those being serviced?

   Followed up on any exceptions outstanding for 120 days or more?

4. Tested impairment analyses?

5. Determined the accuracy of financial reporting systems and other management information systems?

6. Checked compliance with established policies and procedures, accounting recognition, and laws, rules and regulations?

**Bank Dealer Activities**

1. Confirmed securities balances (verification included physical count of securities located at the bank, confirmation of securities held outside the bank or in transit, or testing of internal confirmation and reconciliation process)?

2. Determined the book and market value of trading account securities or tested the internal month-end valuation process?

3. Determined the gain and loss on underwriting and trading account transactions?

4. Reviewed the accrued interest accounts and checked computation of interest income?

5. Confirmed “fails” and “due bills"?

6. Confirmed good faith deposits and cash collateral?

7. Reviewed and tested the bank’s municipal securities dealer department, government securities dealer department, or the bank’s discount broker activity for compliance with applicable laws and regulations (12 USC 24, 15 USC 78o-4, 15 USC 78o-5, and 12 CFR 10 and 12)?

8. Determined that the compliance review is conducted pursuant to comprehensive written audit policies and procedures?

9. Determined that violations or suspected violations of laws, rules, and regulations are referred to the legal counsel for review and that the results of that review are made a part of the audit report to the board or its committee?

**Loans**

Commercial

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Tested the pricing of negotiable collateral?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

Accounts Receivable Financing

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Reviewed the accrued interest accounts and checked computation of interest income?

Direct Lease Financing

1. Confirmed leases and related balance sheet accounts?

2. Reviewed leases and other legal documentation?

3. Tested computation of depreciation expense?

4. Tested computation of interest or rent income?

5. Tested computation of gain or loss on property sales and disposals and traced sales proceeds to cash receipts records?

6. Determined that any deferred tax liability or asset is accurately reflected?

7. Reviewed insurance coverage and determined that property damage coverage is adequate in relation to book value and that liability insurance is in effect?

Installment

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

4. Reviewed unearned discount and any accrued interest balances and tested the computation of interest income?

5. Reviewed sales of repossessed collateral and determined the propriety of the entries made to record the sales?

6. Tested rebate amounts for loans which have been prepaid?

Floor Plan

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation?

3. Physically inspected collateral?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

Credit Card

1. Confirmed loan balances?

2. Tested the computation of interest income?

Home Equity

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation?

3. Tested computation of interest income?

Check Credit

1. Confirmed loan balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation?

3. Tested computation of interest (and service fee, if applicable) income?

Real Estate and Real Estate Construction

1. Confirmed loan and escrow account balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

4. Reviewed the accrued interest accounts and tested computation of interest income?

5. Tested contingency or escrow account balances?

Oil and Gas

1. Confirmed loan balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Reviewed division transfer orders or pipeline companies that have been instructed to remit directly to the bank?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

### Allowance For Loan and Lease Losses

1. Confirmed loan balances for loans charged off since their last examination and amounts of debit entries to the reserve account?

2. Examined supporting documentation for loans charged off?

3. Reviewed loan recoveries and agreed amounts to credit entries in the reserve account?

4. Tested the recording of deferred tax credits (charges) if the deduction for loan losses on the bank's tax return was different from that charged to operations?

### Bank Premises and Equipment

1. Examined support for additions, sales and disposals?

2. Reviewed property transactions with "bank-affiliated personnel"?

3. Verified property balances?

4. Tested computation of depreciation expense?

5. Tested computation of gain or loss on property sales and disposals and traced sales proceeds to cash receipts records?

6. Determined that any deferred tax liability or asset, evolving from the use of different depreciation methods for book and tax purposes, is properly reflected on the bank=s books?

### Other Assets

1. Confirmed other asset balances?

2. Examined support for additions and disposals?

3. Tested the computation of any gains or losses on disposals?

4. Tested the bank's computation of any amortization?

5. Reviewed inter-office transactions?

6. Reviewed suspense accounts to determine whether all items included were temporary?

**Deposits**

Demand and Other Transaction Accounts

1. Confirmed account balances?

2. Tested closed accounts and determined that they were properly closed?

3. Tested account activity in dormant accounts, bank controlled accounts (such as dealers' reserves), employee/officer accounts, and accounts of employees'/officers' business interests?

4. Reviewed overdraft accounts and determined collection potential?

5. Tested computation of service charges and traced postings to appropriate income accounts?

Time Deposit Accounts

1. Confirmed time deposit account balances?

2. Tested closed accounts and determined that they were properly closed?

3. Tested account activity in dormant accounts, bank controlled accounts, employee/officer accounts, and accounts of employees'/officers' business interests?

4. Reviewed the accrued interest accounts and tested computations of interest expense?

5. Accounted for numerical sequence of pre-numbered certificates of deposit?

Official Checks

1. Reconciled account balances?

2. Determined the validity and completeness of outstanding checks?

3. Examined documentation supporting paid checks?

4. Tested certified checks to customer's collected funds balances?

**Borrowed Funds**

1. Confirmed borrowed funds balances?

2. Examined supporting legal documents, disclosures, and collateral custody agreements and determined compliance with applicable laws and regulations?

3. Reviewed minutes of the stockholders' and board of directors' meetings for approval of all borrowing requiring such approval?

4. Verified changes in capital notes outstanding?

5. Reviewed the accrued interest accounts and tested computation of interest expense?

**Other Liabilities**

1. Confirmed balances of "other liability" accounts (including tests for unrecorded liabilities as of a given date)?

2. Reviewed the operation and use of any "inter-office" account?

3. Reviewed suspense accounts to determine all items cleared on a timely basis?

## Capital Accounts and Dividends

Capital Stock

1. If a bank acts as its own transfer agent or registrar, accounted for all stock certificates, (issued and unissued) and reconciled par value of outstanding shares to appropriate general ledger control accounts?

2. If bank has an outside transfer agent or registrar, confirmed shares issued and activity since previous examination?

3. Reviewed capital changes since previous examination?

Dividends

1. Tested the computation of dividends paid or accrued?

2. Reviewed minutes of the board of directors' meetings to determine propriety of dividend payments and accruals?

## Consigned Items and Other Non-Ledger Control Accounts

Safe Deposit Boxes

1. Tested rental income?

2. Checked vault entry records for signature(s) of authorized persons?

3. Tested reconcilements of control records?

Safekeeping/Custodial Accounts

1. Examined or confirmed with outside custodian safekeeping/custodial items?

2. Tested completeness of safekeeping/custodial items and records by examining supporting documentation or by confirming with customers?

3. Tested closed safekeeping/custodial accounts?

4. Tested safekeeping/custodial fee income?

Collection Items

1. Tested collection items by examining supporting documentation, subsequent receipt of payments, disbursement to customers of funds collected, or by confirming with customers?

2. Tested collection fee income?

Consigned Items

1. Reconciled physical count of unissued and voided items on hand to memorandum controls?

2. Confirmed with consignor the inventory on hand at the bank?

3. Tested income from sale of consigned items?

**Income and Expenses**

1. Tested income and expenses by examining supporting documentation for authenticity and proper approval?

2. Tested accruals by either recomputing amounts or examining documents supporting such accruals?

**Related Organizations**

1. Reviewed and tested the investment in and the transactions with related organizations?

2. Determined that investments, advances, or transactions with affiliates are consistent with covenants of debt or other instruments as approved by the board of directors or bank management?

**Information System Services**

1. Performed periodic audit procedures for significant automated applications to determine that workflow is processed accurately and in conformity with operating manuals?

2. Controlled or periodically reviewed dormant accounts?

3. Reviewed unposted items?

**Payment Systems Risk**

1. Tested the bank's self assessment?

2. Reviewed the reasonableness of any de minimis cap?

3. Ascertained compliance with established bank policy?

**Funds Transfer Activities**

1. Reviewed the wire transfer function for segregation of duties involving receipt, processing, settlement, accounting, and reconciling?

2. Tested staff compliance with credit and personnel procedures, operating instructions, and internal controls?

3. Reviewed intraday and overnight overdrafts resulting from fails or intentional extensions of credit?

**Asset Management**

1. Tested fee income and client reimbursement?

2. Examined asset management client contracts?

3. Checked for compliance with applicable laws, regulations and rulings?

4. Ascertained adherence with established bank policies and procedures?

**Private Placements**

1. Tested transactions for evaluation of both issuer and investor, including suitability of the investment?

2. Checked for possible conflicts of interest?

3. Tested the reasonableness of fees charged for loans or paid on deposits?

4. Ascertained that activities are in keeping with established bank policy and SEC rules and regulations?

**Discount Brokerage Activities**

1. Tested transactions for compliance with 12 CFR 12?

2. Reviewed advertising and customer disclosures for accuracy?

3. Tested customer account statements for accuracy?

4. Tested activities for timeliness of processing/transmitting, reliability of accounting records, and for abuses or irregularities?

5. Ascertained compliance with established bank policies and procedures?

**Branches**

1. Has the internal or external auditor performed appropriate audit procedures in the branches during a reasonable audit cycle which are at least as comprehensive as those listed in the applicable areas above?

# References

### Laws

12 USC 1831m, Early Identification of Needed Improvements in Financial Management
12 USC 1831p-1, Standards for Safety and Soundness
15 USC 78m, Periodical and Other Reports

### Regulations

12 CFR 11.2, Requirements under Certain Sections of the Securities Exchange Act of 1934
12 CFR 30, Safety and Soundness Standards
12 CFR 363, Annual Independent Audits and Reporting Requirements
17 CFR 210.1 through 210.4, Form and Content of and Requirements for Financial Statements
17 CFR 229.306, Audit Committee Report
17 CFR 240.14a-101, Schedule 14A, Information Required in Proxy Statement

### OCC Issuances

OCC 98-1, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing"
OCC 99-37, "Interagency Policy Statement on External Auditing Programs"
"The Director's Book: The Role of a National Bank Director"
Federal Financial Institutions Examination Council, *Information Systems Examination Handbook*

### Industry Reference Sources

*AICPA Audit and Accounting Guide, Banks and Savings Institutions*
*AICPA Professional Standards*
AICPA Statement on Auditing Standards:
- 41, "Working Papers", "Providing Access to or Photocopies of Working Papers to a Regulator"
- 55, "Consideration of the Internal Control Structure in a Financial Statement Audit"
- 58, "Reports on Audited Financial Statements"
- 60, "Communication of Internal Control Structure Related Matters Noted in an Audit"

61, "Communication with Audit Committees"
70, "Reports on the Processing of Transactions by Servicing Organizations"
71, "Interim Financial Information"
78, "Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55"
90, "Audit Committee Communications"

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control — Integrated Framework.* Vol. 1, *Executive Summary.* Vol. 2, *Framework.* Vol. 3, *Reporting to External Parties.* Vol. 4, *Evaluation Tools.*

Independence Standards Board
Standard No.1, "Independent Discussions with Audit Committees"
Interpretation 99-1, "FAS 133 Assistance"

The Institute of Internal Auditors, *Codification of Standards for The Professional Practice of Internal Auditing*

*Internal Auditor* (periodical)

New York Stock Exchange, National Association of Securities Dealers, "Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees" (www.nyse.com, www.nasd.com)

Securities and Exchange Commission Staff Accounting Bulletin No.99, "Materiality"

**Web Sites**

AICPA (www.aicpa.org)
Bank Administration Institute (www.bai.org)
Independence Standards Board (www.cpaindependence.org)
Institute of Internal Auditors (www.theiia.org)
OCC Library, Banking and Business (OCC intranet)
Securities and Exchange Commission (www.sec.gov)